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 ist die AWS Lösung, um die Benutzer Ihrer Belegschaft mit AWS verwalteten Anwendungen wie Amazon Q Developer und Amazon Quick Suite sowie anderen AWS Ressourcen zu verbinden. Sie können Ihren bestehenden Identitätsanbieter verbinden und Benutzer und Gruppen aus Ihrem Verzeichnis synchronisieren oder Ihre Benutzer direkt im IAM Identity Center erstellen und verwalten. Anschließend können Sie IAM Identity Center für eine oder beide der folgenden Aufgaben verwenden:

- Benutzerzugriff auf Anwendungen
- Benutzerzugriff auf AWS-Konten

Verwenden Sie IAM bereits für den Zugriff auf? AWS-Konten

Sie müssen keine Änderungen an Ihren aktuellen AWS-Konto Workflows vornehmen, um IAM Identity Center für den Zugriff auf AWS verwaltete Anwendungen zu verwenden. Wenn Sie den Verbund mit IAM für den AWS-Konto Zugriff verwenden, können Ihre Benutzer weiterhin auf die gleiche AWS-Konten Weise zugreifen, wie sie es immer getan haben, und Sie können weiterhin Ihre vorhandenen Workflows verwenden, um diesen Zugriff zu verwalten.

Warum sollten Sie IAM Identity Center verwenden?

IAM Identity Center optimiert und vereinfacht den Benutzerzugriff der Mitarbeiter auf Anwendungen oder AWS-Konten beides durch die folgenden wichtigen Funktionen.

Integration mit verwalteten Anwendungen AWS

AWS verwaltete Anwendungen wie Amazon Q Developer und Amazon Redshift Integration mit IAM Identity Center. IAM Identity Center bietet AWS verwaltete Anwendungen mit einer gemeinsamen Ansicht von Benutzern und Gruppen.

Verbreitung vertrauenswürdiger Identitäten zwischen Anwendungen

Mit Trusted Identity Propagation können AWS verwaltete Anwendungen wie Amazon Quick Suite die Identität eines Benutzers sicher mit anderen AWS verwalteten Anwendungen teilen Amazon Redshift und den Zugriff auf AWS Ressourcen auf der Grundlage der Benutzeridentität autorisieren. Sie können Benutzeraktivitäten einfacher überprüfen, da CloudTrail Ereignisse auf der Grundlage des Benutzers und der vom Benutzer initiierten Aktionen protokolliert werden.

Dadurch lässt sich leichter nachvollziehen, wer auf was zugegriffen hat. Informationen zu unterstützten Anwendungsfällen, einschließlich Anleitungen zur end-to-end Konfiguration, finden Sie unterAnwendungsfälle zur Verbreitung vertrauenswürdiger Identitäten.

Ein Ort, an dem Sie mehreren Benutzern Berechtigungen zuweisen können AWS-Konten

Mit Berechtigungen für mehrere Konten bietet IAM Identity Center einen zentralen Ort, an dem Sie mehreren Benutzergruppen Berechtigungen zuweisen können. AWS-Konten 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 zu kontrollieren AWS-Konten.

Diese optionale Funktion ist nur für Organisationsinstanzen von IAM Identity Center verfügbar.

Ein zentraler Verbundpunkt zur Vereinfachung des Benutzerzugriffs auf AWS

Durch die Bereitstellung eines zentralen Verbundpunkts reduziert IAM Identity Center den Verwaltungsaufwand für die Verwendung mehrerer AWS verwalteter Anwendungen und AWS-Konten. Mit IAM Identity Center können Sie den Verbund nur einmal durchführen, und Sie müssen nur ein Zertifikat verwalten, wenn Sie einen `SAML 2.0`Identitätsanbieter verwenden. IAM Identity Center bietet AWS verwalteten Anwendungen eine gemeinsame Ansicht von Benutzern und Gruppen für Anwendungsfälle zur Verbreitung vertrauenswürdiger Identitäten oder wenn Benutzer den Zugriff auf AWS Ressourcen mit anderen Personen teilen.

Informationen zur Konfiguration häufig verwendeter Identitätsanbieter für die Verwendung mit IAM Identity Center finden Sie unter. Tutorials zu Identitätsquellen im IAM Identity Center Wenn Sie noch keinen Identitätsanbieter haben, können Sie Benutzer direkt in IAM Identity Center erstellen und verwalten.

Zwei Bereitstellungsarten

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 verwalten können AWS.

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.

Benutzerfreundlicher Zugriff auf das Webportal für Ihre Benutzer

Das AWS Zugangsportal ist ein benutzerfreundliches Webportal, das Ihren Benutzern einen nahtlosen Zugriff auf alle ihnen zugewiesenen Anwendungen oder auf beide bietet. AWS-Konten

IAM Identity Center umbenennen

Am 26. Juli 2022 wurde AWS Single Sign-On in umbenannt. AWS IAM Identity Center

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`
- CloudFormationRessourcen, die Präfixe enthalten `AWS::SSO`
- Mit dem Dienst verknüpfte Rolle, die enthält `AWSServiceRoleForSSO`
- Konsole URLs mit und `sso` `singlesignon`
- Dokumentation, URLs die enthält `singlesignon`

Erste Schritte mit IAM Identity Center

Im Folgenden wird beschrieben, wie Sie mit IAM Identity Center beginnen können.

1. IAM Identity Center aktivieren

   Wenn Sie IAM Identity Center aktivieren, können Sie zwischen zwei Arten von IAM Identity Center-Instanzen wählen. Diese Typen sind: Organisationsinstanzen (empfohlen) und Kontoinstanzen. Weitere Informationen zu den verschiedenen Funktionen dieser Instanztypen finden Sie unter Organisations- und Kontoinstanzen von IAM Identity Center.

   > **Note**
   >
   > Nachdem IAM Identity Center aktiviert wurde, können Sie sich anmelden und die IAM Identity Center-Konsole öffnen, indem Sie einen der folgenden Schritte ausführen:
   >
   > - Organisationsinstanz — Melden Sie sich mit AWS Anmeldeinformationen und Administratorrechten im Verwaltungskonto an.
   > - Kontoinstanz — Melden Sie sich mit AWS Anmeldeinformationen und Administratorrechten in dem Bereich an, in AWS-Konto dem IAM Identity Center aktiviert ist.

2. Connect Ihre Identitätsquelle mit dem IAM Identity Center

   Bestätigen Sie in der IAM Identity Center-Konsole die Identitätsquelle, die Sie verwenden möchten. Im Folgenden finden Sie Informationen zu Identitätsquellen:

   - Externer Identitätsanbieter — Wenn Sie bereits über einen Identitätsanbieter zur Verwaltung Ihrer Workforce-Benutzer verfügen, können Sie ihn mit IAM Identity Center verbinden. Weitere Informationen zur Konfiguration häufig verwendeter Identitätsanbieter für die Zusammenarbeit mit IAM Identity Center finden Sie unter. Tutorials zu Identitätsquellen im IAM Identity Center
   - Active Directory — Wenn Sie Active Directory zur Verwaltung Ihrer Workforce-Benutzer verwenden, können Sie es mit dem IAM Identity Center verbinden. Weitere Informationen finden Sie unter Verwenden von Active Directory als Identitätsquelle.
   - IAM Identity Center — Alternativ können Sie Benutzer und Gruppen direkt im IAM Identity Center erstellen und verwalten.

3. Richten Sie den Benutzerzugriff ein für AWS-Konten (nur für die Organisationsinstanz)

Wenn Sie eine Organisationsinstanz von IAM Identity Center verwenden, können Sie Benutzer- oder Gruppenzugriff zuweisen AWS-Konten und Ihren Benutzern mithilfe von Berechtigungssätzen Zugriff auf AWS-Konten und Ressourcen gewähren.

4. Richten Sie Benutzerzugriff auf Anwendungen ein

   Mit IAM Identity Center können Sie Benutzern Zugriff auf zwei Arten von Anwendungen gewähren:

   a. AWS verwaltete Anwendungen
      - Sie können IAM Identity Center mit AWS verwalteten Anwendungen wie Amazon Q Business und Amazon Redshift verwenden. AWS CLI Weitere Informationen erhalten Sie unter AWS verwaltete Anwendungen und Integration von AWS CLI mit IAM Identity Center.

   b. Vom Kunden verwaltete Anwendungen
      - Sie können eine der folgenden Arten von kundenverwalteten Anwendungen in IAM Identity Center integrieren:
        - Anwendungen, die im IAM Identity Center-Katalog aufgeführt sind
        - Ihre benutzerdefinierten Anwendungen
      - Nach der Konfiguration Ihrer Anwendung können Sie Ihren Benutzern Zugriff auf die Anwendung zuweisen.

5. Stellen Sie Ihren Benutzern Anweisungen zur Anmeldung für das AWS Zugangsportal zur Verfügung

   Das AWS Zugriffsportal ist ein Webportal, das Ihren Benutzern nahtlosen Zugriff auf alle ihnen zugewiesenen Anwendungen oder auf beide bietet. AWS-Konten Neue Benutzer in IAM Identity Center müssen ihre Benutzeranmeldedaten aktivieren, bevor sie sich beim AWS Zugriffsportal anmelden können.

   Informationen zur Anmeldung beim AWS Access-Portal finden Sie unter Anmelden im AWS Access-Portal im AWS-Anmeldung Benutzerhandbuch. Weitere Informationen zum Anmeldevorgang für das AWS Access-Portal finden Sie unter Beim AWS Access-Portal anmelden.

Voraussetzungen und Überlegungen zu IAM Identity Center

Sie können IAM Identity Center nur für den Zugriff auf AWS verwaltete Anwendungen, AWS-Konten nur oder für beides verwenden. Wenn Sie den IAM-Verbund zur Verwaltung des Zugriffs auf verwenden AWS-Konten, können Sie dies weiterhin tun und gleichzeitig IAM Identity Center für den Anwendungszugriff verwenden.

Bevor Sie IAM Identity Center aktivieren, sollten Sie Folgendes beachten:

- AWS Region

  Sie können IAM Identity Center für jede Instanz von IAM Identity Center in einer einzelnen unterstützten Region aktivieren. Wenn Sie IAM Identity Center für den Single-Sign-On-Zugriff auf AWS Konten verwenden möchten, muss die Region für alle Benutzer in Ihrer Organisation zugänglich sein. Wenn Sie planen, IAM Identity Center für den Anwendungszugriff zu verwenden, beachten Sie, dass einige AWS verwaltete Anwendungen, wie Amazon SageMaker AI, nur in den Regionen ausgeführt werden können, die sie unterstützen. Stellen Sie sicher, dass Sie IAM Identity Center in einer Region aktivieren, die von den AWS verwalteten Anwendungen unterstützt wird, die Sie damit verwenden möchten. Darüber hinaus können viele AWS verwaltete Anwendungen nur in derselben Region ausgeführt werden, in der Sie IAM Identity Center aktiviert haben. Aus diesen Gründen sollten Sie bei der Aktivierung von IAM Identity Center unbedingt die entsprechende Region auswählen. Weitere Informationen finden Sie unter Überlegungen zur Auswahl eines AWS-Region.

- Nur Anwendungszugriff

  Sie können IAM Identity Center nur für den Benutzerzugriff auf Anwendungen wie Amazon Q Developer verwenden, indem Sie Ihren vorhandenen Identitätsanbieter verwenden. Weitere Informationen finden Sie unter IAM Identity Center nur für den Benutzerzugriff auf Anwendungen verwenden.

  > **Note**
  >
  > Der Zugriff auf Anwendungsressourcen wird unabhängig vom Anwendungseigentümer verwaltet.

- Kontingent für IAM-Rollen

  IAM Identity Center erstellt IAM-Rollen, um Benutzern Berechtigungen für Kontoressourcen zu erteilen. Weitere Informationen finden Sie unter Von IAM Identity Center erstellte IAM-Rollen.

- 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 bereits eingerichtet haben AWS Organizations und zu Ihrer

Organisation hinzufügen möchten, stellen Sie sicher, dass alle AWS Organizations Funktionen aktiviert sind. Weitere Informationen finden Sie unter IAM Identity Center und AWS Organizations.

Überlegungen zur Auswahl eines AWS-Region

Sie können IAM Identity Center in einem einzigen, unterstützten System AWS-Region Ihrer Wahl aktivieren, das Benutzern weltweit zur Verfügung steht. Diese globale Verfügbarkeit erleichtert Ihnen die Konfiguration des Benutzerzugriffs auf mehrere AWS-Konten Anwendungen. Im Folgenden finden Sie wichtige Überlegungen zur Auswahl eines AWS-Region.

- Geografischer Standort Ihrer Benutzer — 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 AI.
- Verfügbarkeit AWS verwalteter Anwendungen — AWS verwaltete Anwendungen können nur in dem Land ausgeführt werden, AWS-Regionen in dem sie verfügbar sind. 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 Ihr selbstverwaltetes Verzeichnis in Active Directory (AD) als Identitätsquelle verwenden AWS Managed Microsoft AD, muss dessen Heimatregion mit der Region übereinstimmen, AWS-Region in der Sie IAM Identity Center aktiviert haben.
- Opt-in-Regionen (Regionen, die standardmäßig deaktiviert sind) — Eine Opt-in-Region ist eine Region AWS-Region , die standardmäßig deaktiviert ist. Um eine Opt-in-Region verwenden zu können, müssen Sie sie aktivieren. Weitere Informationen finden Sie unter Verwaltung des IAM Identity Center in einer Opt-in-Region.
- Regionsübergreifende E-Mails mit Amazon Simple Email Service — In einigen Regionen ruft IAM Identity Center möglicherweise Amazon Simple Email Service (Amazon SES) 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 finden Sie unter Regionsübergreifende E-Mails mit Amazon SES.

Themen

- Datenspeicherung und Betrieb der IAM Identity Center-Region
- Umschalten AWS-Regionen
- Deaktivierung und AWS-Region wo IAM Identity Center aktiviert ist

Datenspeicherung und Betrieb der IAM Identity Center-Region

Erfahren Sie, wie IAM Identity Center die Datenspeicherung und den Betrieb von Daten in allen Bereichen handhabt. AWS-Regionen

Erfahren Sie, wie IAM Identity Center Daten speichert

Wenn Sie IAM Identity Center 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.

Regionsübergreifende E-Mails mit Amazon SES

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.

Regionalcode für das IAM Identity Center	Name der Region für das IAM Identity Center	Amazon SES SES-Regionalcode	Name der Amazon SES SES-Region
ap-east-1	Asien-Pazifik (Hongkong)	ap-northeast-2	Asien-Pazifik (Seoul)
ap-south-2	Asien-Pazifik (Hyderabad)	ap-south-1	Asien-Pazifik (Mumbai)
ap-southeast-4	Asien-Pazifik (Melbourne)	ap-southeast-2	Asien-Pazifik (Sydney)
ap-southeast-5	Asien-Pazifik (Malaysia)	ap-southeast-1	Asien-Pazifik (Singapur)
ap-southeast-7	Asien-Pazifik (Thailand)	ap-northeast-3	Asien-Pazifik (Osaka)
ca-west-1	Kanada West (Calgary)	ca-central-1	Kanada (Zentral)
eu-south-2	Europa (Spain)	eu-west-3	Europa (Paris)
eu-central-2	Europa (Zürich)	eu-central-1	Europa (Frankfurt)
mx-central-1	Mexiko (Zentral)	us-east-2	USA Ost (Ohio)
me-central-1	Naher Osten (VAE)	eu-central-1	Europa (Frankfurt)
us-gov-east-1	AWS GovCloud (USA-Ost)	us-gov-west-1	AWS GovCloud (US-West)

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, aber Sie müssen die folgenden Opt-in-Regionen aktivieren, wenn Sie IAM Identity Center verwenden möchten:

- Afrika (Kapstadt)
- Asien-Pazifik (Hongkong)
- Asien-Pazifik (Hyderabad)
- Asien-Pazifik (Jakarta)
- Asien-Pazifik (Melbourne)
- Asien-Pazifik (Malaysia)
- Asien-Pazifik (Thailand)
- Kanada West (Calgary)
- Europa (Milan)
- Europa (Spain)
- Europa (Zürich)
- Israel (Tel Aviv)
- Mexiko (Zentral)
- Middle East (Bahrain)
- Naher Osten (VAE)

Wenn Sie IAM Identity Center in einer Opt-in-Region bereitstellen, müssen Sie diese Region in allen Konten aktivieren, für die Sie den Zugriff auf IAM Identity Center verwalten möchten. Alle Konten

benötigen diese Konfiguration, unabhängig davon, ob Sie Ressourcen in dieser Region erstellen oder nicht. Sie können eine Region für die aktuellen Konten in Ihrer Organisation aktivieren und müssen diese Aktion wiederholen, wenn Sie neue Konten 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.

> **Note**
>
> Ihr AWS Mitgliedskonto muss der gleichen Region angehören wie die Opt-in-Region, in der sich Ihre IAM Identity Center-Instanz befindet, damit Sie über das Zugriffsportal auf das AWS Mitgliedskonto zugreifen können. AWS

Metadaten, die in Opt-in-Regionen gespeichert sind

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

AWS-Regionen die standardmäßig aktiviert sind

Die folgenden Regionen sind standardmäßig aktiviert, und Sie können IAM Identity Center in diesen Regionen aktivieren.

- 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)

Umschalten AWS-Regionen

Wir empfehlen, dass Sie IAM Identity Center in einer Region installieren, die Sie weiterhin für Benutzer verfügbar halten möchten, und nicht in einer Region, die Sie möglicherweise deaktivieren müssen. Weitere Informationen finden Sie unter Überlegungen zur Auswahl eines AWS-Region.

Sie können Ihre IAM Identity Center-Region nur wechseln, indem Sie Ihre aktuelle IAM Identity Center-Instanz löschen und eine Instanz in einer anderen Region erstellen. Wenn Sie bereits eine AWS verwaltete Anwendung mit Ihrer vorhandenen IAM Identity Center-Instanz aktiviert haben, deaktivieren Sie die Anwendung, bevor Sie IAM Identity Center löschen. Anweisungen zur Deaktivierung AWS verwalteter Anwendungen finden Sie unter. Deaktivierung einer AWS verwalteten Anwendung

Überlegungen zur Konfiguration in der neuen Region

Sie müssen Benutzer, Gruppen, Berechtigungssätze, Anwendungen und Zuweisungen in der neuen IAM Identity Center-Instanz neu erstellen. Sie können das IAM Identity Center-Konto und die Anwendungszuweisung verwenden APIs, um einen Snapshot Ihrer Konfiguration zu erstellen und diesen Snapshot dann verwenden, um Ihre Konfiguration in einer neuen Region neu aufzubauen. Wenn Sie zu einer anderen Region wechseln, ändert sich auch die URL für das AWS Zugriffsportal, das Ihren Benutzern Single-Sign-On-Zugriff auf ihre Anwendungen AWS-Konten bietet.

Möglicherweise müssen Sie auch einige IAM Identity Center-Konfigurationen über die Management Console Ihrer neuen Instanz neu erstellen.

Deaktivierung und AWS-Region wo IAM Identity Center aktiviert ist

Wenn Sie einen deaktivieren, AWS-Region in dem IAM Identity Center installiert ist, ist 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

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.

IAM Identity Center nur für den Benutzerzugriff auf Anwendungen verwenden

Sie können IAM Identity Center für den Benutzerzugriff auf Anwendungen wie Amazon Q Developer oder beides verwenden. AWS-Konten Sie können Ihren vorhandenen Identitätsanbieter verbinden und Benutzer und Gruppen aus Ihrem Verzeichnis synchronisieren oder Benutzer direkt im IAM Identity Center erstellen und verwalten. Informationen darüber, wie Sie Ihren vorhandenen Identitätsanbieter mit IAM Identity Center verbinden, finden Sie unter. Tutorials zu Identitätsquellen im IAM Identity Center

Verwenden Sie IAM bereits für den Zugriff auf? AWS-Konten

Sie müssen keine Änderungen an Ihren aktuellen AWS-Konto Workflows vornehmen, um IAM Identity Center für den Zugriff auf AWS verwaltete Anwendungen zu verwenden. Wenn Sie den Verbund mit IAM für den AWS-Konto Zugriff verwenden, können Ihre Benutzer weiterhin auf die gleiche AWS-

Konten Weise zugreifen, wie sie es immer getan haben, und Sie können weiterhin Ihre vorhandenen Workflows verwenden, um diesen Zugriff zu verwalten.

Von IAM Identity Center erstellte IAM-Rollen

Wenn Sie einem AWS Konto einen Benutzer zuweisen, erstellt IAM Identity Center 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.

> **Note**
>
> Berechtigungssätze werden nicht verwendet, um Anwendungen Berechtigungen zu erteilen.

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 Quota-Benutzerhandbuch.

> **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, 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 Organisationsinstanzen von IAM Identity Center.

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 eine Organisationsinstanz von IAM Identity Center zu aktivieren, müssen Sie sich beim anmelden, AWS-Managementkonsole indem Sie sich mit Ihrem AWS Organizations Verwaltungskonto als Benutzer mit Administratoranmeldedaten oder als Root-Benutzer anmelden (nicht empfohlen, sofern keine anderen Administratorbenutzer vorhanden sind). Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter AWS Organisation erstellen und verwalten.

Wenn Sie mit Administratoranmeldedaten von einem AWS Organizations Mitgliedskonto aus angemeldet sind, können Sie eine Kontoinstanz von IAM Identity Center aktivieren. Kontoinstanzen haben eingeschränkte Funktionen und sind an ein einziges AWS Konto gebunden.

Organisations- und Kontoinstanzen von IAM Identity Center

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

- Organisationsinstanz (empfohlen)

  Eine Instanz von IAM Identity Center, die Sie im AWS Organizations Verwaltungskonto aktivieren. Organisationsinstanzen unterstützen alle Funktionen von IAM Identity Center. Wir empfehlen, eine Organisationsinstanz anstelle von Kontoinstanzen bereitzustellen, um die Anzahl der Verwaltungspunkte zu minimieren.

- Kontoinstanz

  Eine Instanz von IAM Identity Center, die an eine einzelne AWS-Konto Instanz gebunden ist und nur in der AWS-Konto AWS Region sichtbar ist, in der sie aktiviert ist. Verwenden Sie eine Kontoinstanz für einfachere Szenarien mit einem Konto. Sie können eine Kontoinstanz über eine der folgenden Optionen aktivieren:

  - Und AWS-Konto das wird nicht verwaltet von AWS Organizations
  - Ein Mitgliedskonto in AWS Organizations

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-Managementkonsole

- 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 — Verwenden Sie diese Option, 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. Sie können einer eigenständigen Instanz nur eine Instanz von IAM Identity

Center zuordnen AWS-Konto und diese Instanz für Anwendungszuweisungen innerhalb dieser eigenständigen AWS-Konto Instanz verwenden.

Verwenden Sie die folgende Tabelle, um die Funktionen zu vergleichen, die der Instanztyp bietet:

Funktion	Instanz im AWS Organizations Verwaltungskonto (empfohlen)	Instanz in einem Mitgliedskonto	Instanz in einer eigenständigen Instanz AWS-Konto
Benutzer verwalten	 Ja	 Ja	 Ja
AWS Zugriffsportal für Single-Sign-On-Zugriff auf Ihre AWS verwalteten Anwendungen	 Ja	 Ja	 Ja
OAuth 2.0 (OIDC), vom Kunden verwaltete 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

Funktion	Instanz im AWS Organizations Verwaltungskonto (empfohlen)	Instanz in einem Mitgliedskonto	Instanz in einer eigenständigen Instanz AWS-Konto
Ein delegierter Administrator kann die Instanz verwalten	 Ja	 N	 Nein

Weitere Informationen zu AWS verwalteten Anwendungen und IAM Identity Center finden Sie unter. AWS verwaltete Anwendungen, die Sie mit IAM Identity Center verwenden können

Themen

- Organisationsinstanzen von IAM Identity Center
- Kontoinstanzen von IAM Identity Center
- Löschen Sie Ihre IAM Identity Center-Instanz

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.

Informationen zum Aktivieren einer Organisationsinstanz von IAM Identity Center finden Sie unter. Um eine Instanz von IAM Identity Center zu aktivieren

Wann sollte eine Organisationsinstanz verwendet werden

Eine Organisationsinstanz ist die primäre Methode zur Aktivierung von IAM Identity Center. In der Regel 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.
- Reduzierung der 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.
- Zentrale Steuerung der Erstellung von Kontoinstanzen — Sie können steuern, ob Kontoinstanzen von Mitgliedskonten in Ihrer Organisation erstellt werden können, solange Sie in Ihrer Organisation keine Instanz von IAM Identity Center in einer Opt-in-Region bereitgestellt haben (AWS-Region die standardmäßig deaktiviert ist).

Anweisungen zur Aktivierung einer Organisationsinstanz von IAM Identity Center finden Sie unter. Um eine Instanz von IAM Identity Center zu aktivieren

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: einem Mitgliedskonto in AWS Organizations oder einem eigenständigen Konto AWS-Konto , das nicht von verwaltet wird AWS Organizations.

Anweisungen zur Aktivierung einer Kontoinstanz von IAM Identity Center finden Sie unter Um eine Instanz von IAM Identity Center zu aktivieren und wählen Sie den Tab Konto aus.

Wann sollte eine Kontoinstanz verwendet werden

In den meisten Fällen wird eine Organisationsinstanz empfohlen. Verwenden Sie Kontoinstanzen nur, 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.
- Sie haben keine Kontrolle über die AWS Organisation, in der Sie tätig sind. Beispielsweise kontrolliert ein Dritter die AWS Organisation, die Ihre verwaltet AWS-Konten.

> **Important**
>
> Wenn Sie planen, IAM Identity Center zur Unterstützung von Anwendungen in mehreren Konten zu verwenden, verwenden Sie eine Organisationsinstanz. Kontoinstanzen unterstützen diesen Anwendungsfall nicht.

AWS verwaltete Anwendungen, die Kontoinstanzen unterstützen

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

Verfügbarkeitsbeschränkungen für Mitgliedskonten

Um Kontoinstanzen von IAM Identity Center in AWS Organizations Mitgliedskonten bereitzustellen, muss eine der folgenden Bedingungen erfüllt sein:

- In Ihrer Organisation gibt es keine Organisationsinstanz von IAM Identity Center.
- In Ihrer Organisation gibt es eine Organisationsinstanz von IAM Identity Center, und der Instanzadministrator genehmigt die Erstellung von Kontoinstanzen von IAM Identity Center (für Organisationsinstanzen, die nach dem 15. November 2023 erstellt wurden).
- In Ihrer Organisation gibt es eine Organisationsinstanz von IAM Identity Center, und der Instanzadministrator hat die manuelle Erstellung von Kontoinstanzen durch Mitgliedskonten in der Organisation aktiviert (für Organisationsinstanzen, die vor dem 15. November 2023 erstellt wurden). Detaillierte Anweisungen finden Sie unter Erlauben Sie die Erstellung von Kontoinstanzen in Mitgliedskonten.

Wenn eine der oben genannten Bedingungen erfüllt ist, müssen alle der folgenden Bedingungen erfüllt sein:

- 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 von AWS-Region.
- Sie arbeiten in einem Land, in AWS-Region dem IAM Identity Center verfügbar ist. Informationen zu Regionen finden Sie unterDatenspeicherung und Betrieb der IAM Identity Center-Region.

Überlegungen zur Kontoinstanz

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 oder zusammenführen.
- Nur ausgewählte AWS verwaltete Anwendungen unterstützen 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.

Erlauben Sie die Erstellung von Kontoinstanzen in Mitgliedskonten

Wenn Sie IAM Identity Center vor dem 15. November 2023 aktiviert haben, haben Sie eine Organisationsinstanz von IAM Identity Center, bei der die Möglichkeit, dass Mitgliedskonten Kontoinstanzen erstellen können, standardmäßig deaktiviert ist. Sie können wählen, ob Ihre Mitgliedskonten Kontoinstanzen erstellen können, indem Sie die Kontoinstanzfunktion in der IAM Identity Center-Konsole aktivieren.

Um die Erstellung von Kontoinstanzen durch Mitgliedskonten in Ihrer Organisation zu ermöglichen

> **Important**
>
> Die Aktivierung 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.

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.

Verwenden Sie Service Control-Richtlinien, um die Erstellung von Kontoinstanzen zu steuern

Ob Mitgliedskonten Kontoinstanzen erstellen können, hängt davon ab, wann Sie IAM Identity Center aktiviert haben:

- Vor November 2023 — Sie müssen die Erstellung von Kontoinstanzen in Mitgliedskonten zulassen. Diese Aktion kann nicht rückgängig gemacht werden.
- Nach dem 15. November 2023 — Mitgliedskonten können standardmäßig Kontoinstanzen erstellen.

In beiden Fällen können Sie Service Control Policies (SCPs) verwenden, um:

- Verhindern Sie, dass alle Mitgliedskonten Kontoinstanzen erstellen.
- Erlauben Sie nur bestimmten Mitgliedskonten, Kontoinstanzen zu erstellen.

Kontoinstanzen verhindern

Gehen Sie wie folgt vor, um einen SCP zu generieren, der verhindert, dass Mitgliedskonten Kontoinstanzen von IAM Identity Center erstellen.

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

Beschränken Sie Kontoinstanzen

Anstatt die Erstellung aller Kontoinstanzen zu verhindern, verbietet diese Richtlinie jeden Versuch, eine Kontoinstanz von IAM Identity Center für alle zu erstellen, AWS-Konten mit Ausnahme der *"<ALLOWED-ACCOUNT-ID>"* explizit im Platzhalter aufgeführten.

Example : Richtlinie zur Beschränkung der Erstellung von Kontoinstanzen ablehnen

JSON

```
{

    "Version":"2012-10-17",
    "Statement" : [
        {
            "Sid": "DenyMemberAccountInstances",
            "Effect": "Deny",
            "Action": "sso:CreateInstance",
            "Resource": "*",
            "Condition": {
                 "StringNotEquals": {
                    "aws:PrincipalAccount": ["<ALLOWED-ACCOUNT-ID>"]
                }
            }
```

```
        }
    ]
}
```

- Ersetzen Sie ["*<ALLOWED-ACCOUNT-ID>*"] durch die tatsächlichen AWS-Konto IDs, denen Sie die Erstellung einer Kontoinstanz von IAM Identity Center erlauben möchten.
- Sie können mehrere zulässige Konten IDs im Array-Format auflisten: [*"111122223333", "444455556666"*].
- Fügen Sie diese Richtlinie dem SCP Ihrer Organisation bei, um eine zentrale Kontrolle über die Erstellung von IAM Identity Center-Kontoinstanzen durchzusetzen.

  Anweisungen zum Anhängen eines SCP finden Sie im Benutzerhandbuch unter Dienststeuerungsrichtlinien anhängen und trennen.AWS Organizations

Löschen Sie Ihre IAM Identity Center-Instanz

Wenn eine IAM Identity Center-Instanz gelöscht wird, werden alle Daten in dieser Instanz gelöscht und können nicht wiederhergestellt werden. In der folgenden Tabelle wird beschrieben, welche Daten basierend auf dem Verzeichnistyp, der in IAM Identity Center konfiguriert ist, gelöscht werden.

Welche Daten werden gelöscht	Verbundenes Verzeichnis — AWS Managed Microsoft AD, AD Connector oder externer Identitätsanbieter	IAM Identity Center-Identitätsspeicher	
Alle Berechtigungssätze, für die Sie konfiguriert haben AWS-Konten	 Ja	 Ja	
Alle Anwendungen, die Sie in IAM Identity Center konfiguriert haben	 Ja	 Ja	

Welche Daten werden gelöscht	Verbundenes Verzeichnis — AWS Managed Microsoft AD, AD Connector oder externer Identitätsanbieter	IAM Identity Center-Identitätsspeicher	
Alle Benutzerzuweisungen, für die Sie konfiguriert haben, AWS-Konten und alle Anwendungen	 Ja		Ja
Alle Benutzer und Gruppen im Verzeichnis oder Speicher	N/A		Ja

Gehen Sie wie folgt vor, um Ihre IAM Identity Center-Instanz zu löschen.

Um Ihre IAM Identity Center-Instanz 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 aus.
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 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.

IAM Identity Center aktivieren

Wenn Sie IAM Identity Center aktivieren, wählen Sie einen AWS IAM Identity Center Instanztyp aus, den Sie aktivieren möchten. Eine Instanz eines Dienstes ist eine einzelne Bereitstellung eines Dienstes in Ihrer AWS Umgebung. Für IAM Identity Center sind zwei Arten von Instanzen verfügbar: Organisationsinstanzen und Kontoinstanzen. Welche Instance-Typen Sie aktivieren können, hängt vom Kontotyp ab, bei dem Sie angemeldet sind.

In der folgenden Liste sind die Typen der IAM Identity Center-Instanzen aufgeführt, die Sie für jeden Typ aktivieren können: AWS-Konto

- 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 — Verwenden Sie diese Option, 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. Sie können einer eigenständigen Instanz nur eine Instanz von IAM Identity Center zuordnen AWS-Konto und diese Instanz für Anwendungszuweisungen innerhalb dieser eigenständigen AWS-Konto Instanz verwenden.

> **Important**
>
> Das Organisationsverwaltungskonto kann mithilfe einer Service Control-Richtlinie steuern, ob Mitgliedskonten der Organisation Kontoinstanzen von IAM Identity Center erstellen können.

Einen Vergleich der verschiedenen Funktionen, die von den verschiedenen Instanztypen bereitgestellt werden, finden Sie unterOrganisations- und Kontoinstanzen von IAM Identity Center.

Bevor Sie IAM Identity Center aktivieren, empfehlen wir Ihnen, die Voraussetzungen und Überlegungen zu IAM Identity Center zu lesen.

Um eine Instanz von IAM Identity Center zu aktivieren

Wählen Sie die Registerkarte für den Typ der IAM Identity Center-Instanz, die Sie aktivieren möchten, entweder eine Organisations- oder eine Kontoinstanz:

Organization (recommended)

1. Führen Sie einen der folgenden Schritte aus, um sich bei der AWS-Managementkonsole 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 AWS bereits eine eigenständige Version AWS-Konto (IAM-Anmeldeinformationen) — Melden Sie sich mit Ihren IAM-Anmeldeinformationen und Administratorrechten an.
   - Verwenden Sie bereits AWS Organizations (IAM-Anmeldeinformationen) — Melden Sie sich mit den Anmeldeinformationen Ihres Verwaltungskontos an.
2. Öffnen Sie die IAM-Identity-Center-Konsole.
3. (Optional) Wenn Sie anstelle des standardmäßigen AWS verwalteten Schlüssels einen vom Kunden verwalteten KMS-Schlüssel für die Verschlüsselung im Ruhezustand verwenden möchten, konfigurieren Sie den vom Kunden verwalteten Schlüssel im Abschnitt Schlüssel zur Verschlüsselung von IAM Identity Center-Daten im Ruhezustand. Weitere Informationen finden Sie unter Implementierung von vom Kunden verwalteten KMS-Schlüsseln in AWS IAM Identity Center.

   > **Important**
   >
   > Führen Sie diesen Schritt nur aus, wenn Sie die erforderlichen Berechtigungen für die Verwendung des kundenverwalteten KMS-Schlüssels konfiguriert haben. Ohne die entsprechenden Berechtigungen kann dieser Schritt fehlschlagen oder die Verwaltung von IAM Identity Center und die AWS verwalteten Anwendungen unterbrechen.
4. Wählen Sie unter IAM Identity Center aktivieren die Option Aktivieren aus.
5. Überprüfen Sie auf der AWS Organizations Seite „IAM Identity Center aktivieren mit“ die Informationen und wählen Sie dann Aktivieren aus, um den Vorgang abzuschließen.

> **Note**
>
> AWS Organizations kann IAM Identity Center nur in einer einzigen AWS Region aktiviert haben. Wenn Sie nach der Aktivierung von IAM Identity Center die Region ändern möchten, in der IAM Identity Center aktiviert ist, müssen Sie die aktuelle Instanz löschen und eine Instanz in der anderen Region erstellen.

Wir empfehlen Ihnen, nach der Aktivierung Ihrer Organisationsinstanz die folgenden Schritte durchzuführen, um die Einrichtung Ihrer Umgebung abzuschließen:

- Vergewissern Sie sich, dass Sie die Identitätsquelle Ihrer Wahl verwenden. Wenn Ihnen bereits eine Identitätsquelle zugewiesen wurde, können Sie diese weiterhin verwenden. Weitere Informationen finden Sie unter Bestätigen Sie Ihre Identitätsquellen im IAM Identity Center.
- Registrieren Sie ein Mitgliedskonto als delegierter Administrator. Weitere Informationen finden Sie unter Delegierte Verwaltung.
- Das IAM Identity Center bietet Ihnen ein Zugriffsportal zu AWS Ressourcen. Informationen zum Filtern des Zugriffs 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) finden Sie unter. Aktualisieren Sie Firewalls und Gateways, um den Zugriff auf die AWS-Zugangsportal

Account

1. Führen Sie einen der folgenden Schritte aus, um sich bei der anzumelden AWS-Managementkonsole.
   - 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.
   - Verwenden Sie bereits AWS Organizations (IAM-Anmeldeinformationen) — Melden Sie sich mit den Administratordaten Ihres Mitgliedskontos an.
2. Öffnen Sie die IAM-Identity-Center-Konsole.

3. Wenn Sie neu bei IAM Identity Center sind AWS oder über ein eigenständiges System verfügen AWS-Konto, wählen Sie unter IAM Identity Center aktivieren die Option Aktivieren aus.

   Die Seite „IAM Identity Center aktivieren mit AWS Organizations“ wird angezeigt. Wir empfehlen diese Option, sie ist jedoch nicht erforderlich.

   Wählen Sie den Link Eine Kontoinstanz von IAM Identity Center aktivieren aus.

4. Wenn Sie Administrator eines AWS Organizations Mitgliedskontos sind, wählen Sie unter Eine Kontoinstanz von IAM Identity Center aktivieren die Option Kontoinstanz aktivieren aus.

5. Überprüfen Sie auf der Seite Eine Kontoinstanz von IAM Identity Center aktivieren die Informationen und fügen Sie optional Tags hinzu, die Sie dieser Kontoinstanz zuordnen möchten. Wählen Sie dann Aktivieren aus, um den Vorgang abzuschließen.

> **Note**
>
> Wenn Ihr AWS Konto Mitglied einer Organisation ist, sind Ihre Möglichkeiten, eine Kontoinstanz von IAM Identity Center zu aktivieren, möglicherweise eingeschränkt.
>
> - Wenn Ihre Organisation IAM Identity Center vor dem 15. November 2023 aktiviert hat, ist die Möglichkeit für Mitgliedskonten, Kontoinstanzen zu erstellen, standardmäßig deaktiviert und muss durch das Verwaltungskonto der Organisation aktiviert werden.
> - Wenn Ihre Organisation IAM Identity Center nach dem 15. November 2023 aktiviert hat, ist die Möglichkeit für Mitgliedskonten, Kontoinstanzen zu erstellen, standardmäßig aktiviert. Richtlinien zur Dienststeuerung können jedoch verwendet werden, um die Erstellung von Kontoinstanzen von IAM Identity Center innerhalb einer Organisation zu verhindern.
>
> Weitere Informationen erhalten Sie unter the section called “Erlauben Sie die Erstellung von Kontoinstanzen in Mitgliedskonten” und the section called “SCPs für die Erstellung einer Kontoinstanz”.

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. Wenn Ihnen bereits eine Identitätsquelle zugewiesen wurde, können Sie diese weiterhin verwenden.

Wenn Sie bereits Benutzer und Gruppen in Active Directory oder einem externen IdP verwalten, empfehlen wir Ihnen, eine Verbindung zu dieser Identitätsquelle in Betracht zu ziehen, wenn Sie IAM Identity Center aktivieren und Ihre Identitätsquelle auswählen. 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 zur Änderung Ihrer Identitätsquelle.

To confirm your identity source

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 die Registerkarte 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, das Sie 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 Microsoft ADVerzeichnis.

> **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 unterTutorials zu Identitätsquellen im IAM Identity Center.

> **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 Identitätsanbieter nicht unterstützt. Weitere Informationen finden Sie unter Benutzer zur MFA auffordern.

Aktualisieren Sie Firewalls und Gateways, um den Zugriff auf die AWS-Zugangsportal

Das AWS Zugriffsportal bietet Benutzern 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.

> **Note**
>
> AWS verwaltete Anwendungen lassen sich in IAM Identity Center integrieren und verwenden es für Authentifizierungs- und Verzeichnisdienste, verwenden jedoch möglicherweise nicht das AWS Zugriffsportal für den Anwendungszugriff.

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 Domänen und URL-Endpunkte, die dem Zugriffsportal zugeordnet sind, auf eine Zulassungsliste setzen. AWS

Die folgende Liste enthält die Domänen und URL-Endpunkte, die Sie zu den Zulassungslisten Ihrer Lösung zur Filterung von Webinhalten hinzufügen können.

- *[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]*.prod.pr.panorama.console.api.aws/panoramaroute
- *[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

Zusätzlich zu den Zulassungslistenanforderungen für das AWS Zugriffsportal ist für die anderen Dienste und Anwendungen, die Sie verwenden, möglicherweise eine Zulassung von Domänen erforderlich.

- Um von Ihrem AWS-Konten Zugriffsportal aus auf die IAM Identity Center-Konsole und die IAM Identity Center-Konsole AWS zugreifen zu können, müssen Sie zusätzliche Domänen zulassen. AWS-Managementkonsole Eine Liste der Domänen finden Sie im Handbuch AWS-Managementkonsole Erste Schritte unter Problembehandlung. AWS-Managementkonsole
- 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.
- Wenn Sie externe Software verwenden, z. B. externe Software IdPs (z. B. Okta undMicrosoft Entra ID), müssen Sie deren Domänen in Ihre Zulassungslisten aufnehmen.

Tutorials zu Identitätsquellen im IAM Identity Center

Sie können Ihre bestehende Identitätsquelle in Ihrem AWS Organizations Verwaltungskonto mit einer Organisationsinstanz von IAM Identity Center verbinden. Wenn Sie noch keinen Identitätsanbieter haben, können Sie Benutzer direkt im standardmäßigen IAM Identity Center-Verzeichnis erstellen und verwalten. Sie können eine Identitätsquelle pro Organisation haben.

In den Tutorials in diesem Abschnitt wird beschrieben, wie Sie eine Organisationsinstanz von IAM Identity Center mit einer häufig verwendeten Identitätsquelle einrichten, einen Administratorbenutzer erstellen und ob Sie IAM Identity Center verwenden, um den Zugriff zu verwalten AWS-Konten, Berechtigungssätze zu erstellen und zu konfigurieren. Wenn Sie IAM Identity Center nur für den Anwendungszugriff verwenden, müssen Sie keine Berechtigungssätze verwenden.

In diesen Tutorials wird nicht beschrieben, wie Kontoinstanzen von IAM Identity Center eingerichtet werden. Sie können Kontoinstanzen verwenden, um Benutzern und Gruppen Anwendungen zuzuweisen, aber Sie können diesen Instanztyp nicht verwenden, um den Benutzerzugriff auf diese zu AWS-Konten verwalten. Weitere Informationen finden Sie unter Kontoinstanzen von IAM Identity Center.

> **Note**
>
> Bevor Sie mit einem dieser Tutorials beginnen, aktivieren Sie IAM Identity Center. Weitere Informationen finden Sie unter IAM Identity Center aktivieren.

Themen

- Benutzerzugriff mit dem standardmäßigen IAM Identity Center-Verzeichnis konfigurieren
- Video-Tutorials

Verwenden von Active Directory als Identitätsquelle

Wenn Sie Benutzer in Ihrem AWS Managed Microsoft AD Verzeichnis mithilfe von Active Directory (AD) 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 verwenden AWS Managed Microsoft AD, müssen Sie es dort aktivieren AWS-Region , wo Ihr AWS Managed Microsoft AD Verzeichnis eingerichtet ist. IAM Identity Center speichert die Zuweisungsdaten in derselben Region wie das Verzeichnis. Um IAM Identity Center zu verwalten, müssen Sie möglicherweise zu der Region wechseln, in der IAM Identity Center konfiguriert ist. Beachten Sie außerdem, dass das AWS Zugriffsportal dieselbe Zugriffs-URL wie Ihr Verzeichnis verwendet.
- Verwenden Sie ein Active Directory, das sich im Verwaltungskonto befindet:

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

  - Ein Verzeichnis mit dem IAM Identity Center Connect AWS Managed Microsoft AD
  - Ein selbstverwaltetes Verzeichnis in Active Directory mit IAM Identity Center Connect
- 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**
>
> Wenn Sie beabsichtigen, ein AWS Managed Microsoft AD Verzeichnis oder ein selbstverwaltetes Verzeichnis in Active Directory zu verbinden und Sie RADIUS MFA nicht mit verwenden AWS Directory Service, aktivieren Sie MFA in IAM Identity Center.

AWS Managed Microsoft AD

1. Lesen Sie die Anleitung unter. Microsoft ADVerzeichnis
2. Führen Sie die Schritte unter Ein Verzeichnis mit dem IAM Identity Center Connect AWS Managed Microsoft AD 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 Sie einen Administratorbenutzer mit IAM Identity Center.

Selbstverwaltetes Verzeichnis in Active Directory

1. Lesen Sie die Anleitung unterMicrosoft ADVerzeichnis.
2. Führen Sie die Schritte unter Ein selbstverwaltetes Verzeichnis in Active Directory mit IAM Identity Center Connect 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 Sie einen Administratorbenutzer 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 Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“, klicken Sie auf „Aktionen“ und anschließend auf „Synchronisation verwalten“.
4. Wählen Sie auf der Seite „Synchronisation verwalten“ die Registerkarte „Benutzer“ und dann „Benutzer und Gruppen hinzufügen“ aus.
5. Geben Sie auf der Registerkarte Benutzer unter Benutzer den genauen Benutzernamen ein und wählen Sie Hinzufügen aus.
6. Gehen Sie unter Hinzugefügte Benutzer und Gruppen wie folgt vor:
    a. Vergewissern Sie sich, dass der Benutzer, dem Sie Administratorrechte gewähren möchten, angegeben ist.
    b. Aktivieren Sie das Kontrollkästchen links neben dem Benutzernamen.
    c. Wählen Sie Absenden aus.
7. Auf der Seite „Synchronisation verwalten“ wird der von Ihnen angegebene Benutzer in der Liste „Synchronisierte Benutzer“ angezeigt.
8. Klicken Sie im Navigationsbereich auf Users (Benutzer).
9. Auf der Seite Benutzer kann es einige Zeit dauern, bis der von Ihnen angegebene Benutzer in der Liste erscheint. Wählen Sie das Aktualisierungssymbol, um die Benutzerliste zu aktualisieren.

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

Setting up SCIM provisioning between CyberArk and IAM Identity Center

IAM Identity Center unterstützt die automatische Bereitstellung (Synchronisation) von Benutzerinformationen von CyberArk Directory Platform in das IAM Identity Center. Bei dieser Bereitstellung wird das SCIM-Protokoll (System for Cross-Domain Identity Management) v2.0 verwendet. Weitere Informationen finden Sie unter Verwenden des SAML- und SCIM-Identitätsverbunds mit externen Identitätsanbietern.

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. Dadurch stimmen die erwarteten Attribute zwischen IAM Identity Center und CyberArk.

Dieser Leitfaden basiert auf CyberArk 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 lesen. Überlegungen zur Verwendung der automatischen Bereitstellung Lesen Sie dann im nächsten Abschnitt weitere Überlegungen durch.

Themen

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 für das IAM Identity Center, wie unter beschrieben CyberArk Dokumentation für IAM Identity Center.
- Ordnen Sie den IAM Identity Center-Connector den Rollen, Benutzern und Organisationen zu, denen Sie Zugriff gewähren möchten. AWS-Konten

Überlegungen zu SCIM

Folgendes sollten Sie bei der Verwendung von CyberArk Verbund für IAM Identity Center:

- Nur Rollen, die im Abschnitt Anwendungsbereitstellung zugeordnet sind, werden mit IAM Identity Center synchronisiert.
- Das Provisioning-Skript wird nur in seinem Standardstatus unterstützt. Sobald es geändert wurde, schlägt das SCIM-Provisioning möglicherweise fehl.
  - Es kann nur ein Telefonnummernattribut synchronisiert werden, und die Standardeinstellung ist „Geschäftstelefon“.
- Wenn die Rollenzuweisung in CyberArk Die IAM Identity Center-Anwendung wird geändert, und das folgende Verhalten wird erwartet:
  - Wenn die Rollennamen geändert werden — keine Änderungen an den Gruppennamen in IAM Identity Center.
  - Wenn die Gruppennamen geändert werden, werden neue Gruppen in IAM Identity Center erstellt. Alte Gruppen bleiben bestehen, haben aber keine Mitglieder.
- Die Benutzersynchronisierung und das Verhalten bei der Deprovisionierung können im CyberArk Stellen Sie mit der IAM Identity Center-Anwendung sicher, dass Sie das richtige Verhalten für Ihr Unternehmen einrichten. Dies sind die Optionen, die Ihnen zur Verfügung stehen:
  - Benutzer im Identity Center-Verzeichnis mit demselben Prinzipalnamen überschreiben (oder nicht).

- Heben Sie die Benutzerbereitstellung von IAM Identity Center auf, wenn der Benutzer aus dem CyberArk Rolle.
- Benutzerverhalten aufheben — deaktivieren oder löschen.

Schritt 1: Aktivieren Sie die Bereitstellung im IAM Identity Center

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

Um die automatische Bereitstellung in 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 den SCIM-Endpunkt und das Zugriffstoken. Sie müssen diese später einfügen, wenn Sie die Bereitstellung in Ihrem IdP konfigurieren.

   a. SCIM-Endpunkt — Zum Beispiel https://scim. *us-east-2*.amazonaws.com/ /scim/v2 *11111111111-2222-3333-4444-555555555555*

   b. Zugriffstoken — Wählen Sie Token anzeigen, um den Wert zu kopieren.

   > **Warning**
   >
   > Dies ist das einzige Mal, dass Sie den SCIM-Endpunkt und das Zugriffstoken abrufen können. Stellen Sie sicher, dass Sie diese Werte kopieren, bevor Sie fortfahren. Sie werden diese Werte eingeben, um die automatische Bereitstellung in Ihrem IdP später in diesem Tutorial zu konfigurieren.

5. Klicken Sie auf Schließen.

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

Schritt 2: Konfigurieren Sie die Bereitstellung in CyberArk

Verwenden Sie das folgende Verfahren in der CyberArk IAM Identity Center-Anwendung, um die Bereitstellung mit IAM Identity Center zu ermöglichen. Bei diesem Verfahren wird davon ausgegangen, dass Sie das bereits hinzugefügt haben CyberArk IAM Identity Center-Anwendung zu Ihrer CyberArk Admin-Konsole unter Web-Apps. Falls Sie dies noch nicht getan haben, finden Sie weitere Informationen unterVoraussetzungen, und führen Sie dann dieses Verfahren aus, um die SCIM-Bereitstellung zu konfigurieren.

So konfigurieren Sie die Bereitstellung in CyberArk

1. Öffnen Sie 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 Provisioning.
3. Markieren Sie das Kästchen „Bereitstellung für diese Anwendung aktivieren“ und wählen Sie „Live-Modus“.
4. Im vorherigen Verfahren haben Sie den SCIM-Endpunktwert aus dem IAM Identity Center kopiert. Fügen Sie diesen Wert in das Feld SCIM-Dienst-URL ein, im CyberArk Die IAM Identity Center-Anwendung hat den Autorisierungstyp auf Authorization Header festgelegt.
5. Stellen Sie den Header-Typ auf Bearer-Token ein.
6. Aus dem vorherigen Verfahren haben Sie den Wert des Zugriffstokens in IAM Identity Center kopiert. Fügen Sie diesen Wert in das Feld Bearer-Token im CyberArk IAM Identity Center-Anwendung.
7. Klicken Sie auf Überprüfen, um die Konfiguration zu testen und anzuwenden.
8. Wählen Sie unter den Synchronisierungsoptionen das richtige Verhalten aus, für das die ausgehende Bereitstellung erfolgen soll CyberArk um zu arbeiten. Sie können festlegen, ob bestehende IAM Identity Center-Benutzer mit einem ähnlichen Prinzipalnamen und dem Verhalten bei der Deprovisionierung überschrieben werden sollen (oder nicht).
9. Richten Sie unter Rollenzuordnung die Zuordnung von ein CyberArk Rollen, unter dem Feld Name zur IAM Identity Center-Gruppe, unter der Zielgruppe.
10. Wenn Sie fertig sind, klicken Sie unten auf Speichern.

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 wird auf der Benutzerseite angezeigt. Diese Benutzer können jetzt Konten zugewiesen werden und können sich innerhalb von IAM Identity Center verbinden.

(Optional) Schritt 3: Konfigurieren Sie Benutzerattribute in CyberArk für die Zugriffskontrolle (ABAC) im IAM Identity Center

Dies ist ein optionales Verfahren für CyberArk sollten Sie sich dafür entscheiden, Attribute für IAM Identity Center zu konfigurieren, um den Zugriff auf Ihre AWS Ressourcen zu verwalten. Die Attribute, die Sie definieren in CyberArk werden in einer SAML-Assertion an IAM Identity Center übergeben. Anschließend erstellen Sie in IAM Identity Center einen Berechtigungssatz, um den Zugriff auf der Grundlage der Attribute zu verwalten, von denen Sie übergeben haben CyberArk.

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.

Um Benutzerattribute zu konfigurieren CyberArk für die Zugriffskontrolle im IAM Identity Center

1. Öffnen Sie 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 die relevanten Attribute zur Tabelle hinzu. Folgen Sie dabei der folgenden Logik:

   a. Attributname ist der ursprüngliche Attributname von CyberArk.

   b. Attributwert ist der Attributname, der in der SAML-Assertion an IAM Identity Center gesendet wird.
4. Wählen Sie Speichern.

(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.

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 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 2.0-Protokolls (System for Cross-Domain Identity Management) mit IAM Identity Center synchronisiert. Weitere Informationen finden Sie unter Verwenden des SAML- und SCIM-Identitätsverbunds mit externen Identitätsanbietern.

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 Google Workspace als Identitätsanbieter einrichten und eine Verbindung zu Ihrem IAM Identity Center herstellen.

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 in diesem Tutorial nicht enthalten. Nach Abschluss dieses Tutorials können Ihre Benutzer mit Ihren Google Workspace Anmeldeinformationen auf das AWS Zugriffsportal 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 unterIAM Identity Center aktivieren.

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, die mehrere Werte haben, 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 “Wechsel 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 die folgenden Schritte 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 IAM Identity Assertion Consumer Service (ACS) -URL 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 ACS-URL und die Entitäts-ID 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.
9. Füllen Sie auf der Seite mit den Service Provider-Details die Felder unter Name ID wie folgt aus:

   - Wählen Sie für das Namens-ID-Format die Option E-MAIL
   - 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“.

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 zu 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

   a. SCIM-Endpunkt — Zum Beispiel https://scim. *us-east-2*.amazonaws.com/ /scim/v2 *11111111111-2222-3333-4444-555555555555*

   b. Zugriffstoken — Wählen Sie Token anzeigen, um den Wert zu kopieren.

   > **Warning**
   >
   > Dies ist das einzige Mal, dass Sie den SCIM-Endpunkt und das Zugriffstoken abrufen 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 und wählen Sie Weiter.
3. Stellen Sie sicher, dass alle obligatorischen IAM Identity Center-Attribute (die mit einem* markierten) Attributen zugeordnet Google Cloud Directory sind. 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 Deprovisionierung 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, kann es sein, dass die Bereitstellung noch im Gange ist. 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.

Übergabe von Attributen für die Zugriffskontrolle — optional

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.

Weisen Sie Zugriff zu AWS-Konten

Die folgenden Schritte sind nur erforderlich, um AWS-Konten nur Zugriff zu gewähren. Diese Schritte sind nicht erforderlich, um Zugriff auf AWS Anwendungen zu gewähren.

> **Note**
>
> Um diesen Schritt abzuschließen, benötigen Sie eine Organisationsinstanz von IAM Identity Center. Weitere Informationen finden Sie unter Organisations- und Kontoinstanzen von IAM Identity Center.

Schritt 1: 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 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 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.

   iii. Stellen Sie für Schritt 3: Überprüfen und erstellen sicher, dass der Typ Berechtigungssatz die AWS verwaltete Richtlinie verwendet AdministratorAccess. Wählen Sie Erstellen aus. 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-Managementkonsole Nach der Bereitstellung von Benutzern können Sie Gruppen mit dem AWS CLI Identity Store-Befehl create-group oder der IAM-API erstellen. CreateGroup

Schritt 2Google 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 in der Apps-Liste ganz nach unten, wo sich Ihre benutzerdefinierten Google Workspace Apps befinden. Die Amazon Web Services Services-App wird angezeigt.
4. Wählen Sie die Amazon Web Services Services-App aus. Sie sind im AWS Zugangsportal angemeldet und können das AWS-Konto Symbol sehen. Erweitern Sie dieses Symbol, um die Liste der Elemente zu sehen 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.
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-Managementkonsole

7. Der Benutzer ist an der Konsole angemeldet.

Nächste Schritte

Nachdem Sie die Konfiguration Google Workspace als Identitätsanbieter vorgenommen 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, bei dem ein älteres Zertifikat durch ein neueres ersetzt wird, wird als Zertifikatsrotation bezeichnet. Lesen Sie unbedingt, wie Sie die SAML-Zertifikate für Google Workspace verwalten.

Fehlerbehebung

Informationen zur allgemeinen SCIM- und SAML-Problembehandlung mit Google Workspace finden Sie in den folgenden Abschnitten:

- Bestimmte Benutzer können sich von einem externen SCIM-Anbieter nicht mit dem IAM Identity Center synchronisieren
- Probleme mit dem Inhalt von SAML-Assertionen, die von IAM Identity Center erstellt wurden
- Beim Bereitstellen von Benutzern oder Gruppen mit einem externen Identitätsanbieter ist ein Fehler beim Duplizieren von Benutzern oder Gruppen aufgetreten
- Informationen zur Google Workspace Fehlerbehebung finden Sie in der DokumentationGoogle Workspace.

Die folgenden Ressourcen können Ihnen bei der Problembehebung bei der Arbeit mit helfen AWS:

- AWS re:Post- Hier finden Sie weitere Ressourcen FAQs und Links zu diesen, die Ihnen bei der Behebung von Problemen helfen.
- AWS Support- Holen Sie sich technischen Support

Verwenden Sie IAM Identity Center, um sich mit Ihrem zu verbinden JumpCloud Verzeichnis-Plattform

IAM Identity Center unterstützt die automatische Bereitstellung (Synchronisation) von Benutzerinformationen von JumpCloud Verzeichnisplattform in IAM Identity Center. Bei dieser Bereitstellung wird das SAML 2.0-Protokoll (Security Assertion Markup Language) verwendet. Weitere Informationen finden Sie unter Verwenden des SAML- und SCIM-Identitätsverbunds mit externen Identitätsanbietern.

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. Dadurch stimmen die erwarteten Attribute zwischen IAM Identity Center und überein JumpCloud.

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

In den folgenden Schritten erfahren Sie, wie Sie die automatische Bereitstellung von Benutzern und Gruppen von aktivieren JumpCloud über das SCIM-Protokoll zu IAM Identity Center.

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

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 für das IAM Identity Center, wie unter beschrieben JumpCloud Dokumentation für IAM Identity Center.
- Ordnen Sie den IAM Identity Center-Connector den Gruppen zu, denen Sie Zugriff auf Konten gewähren möchten. AWS

Überlegungen zu SCIM

Folgendes sollten Sie bei der Verwendung von JumpCloud Verbund für IAM Identity Center.

- Nur Gruppen, die dem AWS Single Sign-On-Connector zugeordnet sind, in JumpCloud wird mit SCIM synchronisiert.

- Es kann nur ein Telefonnummernattribut synchronisiert werden. Die Standardeinstellung ist „Geschäftstelefon“.
- Benutzer in JumpCloud Im Verzeichnis müssen Vor- und Nachnamen so konfiguriert sein, dass sie mit dem IAM Identity Center mit SCIM synchronisiert werden.
- Attribute werden weiterhin synchronisiert, wenn der Benutzer in IAM Identity Center deaktiviert, aber dennoch aktiviert ist JumpCloud.
- Sie können die SCIM-Synchronisierung nur für Benutzerinformationen aktivieren, indem Sie im Connector die Option „Verwaltung von Benutzergruppen und Gruppenmitgliedschaft aktivieren“ deaktivieren.

Schritt 1: Aktivieren Sie die Bereitstellung im IAM Identity Center

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

Um die automatische Bereitstellung in 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 den SCIM-Endpunkt und das Zugriffstoken. Sie müssen diese später einfügen, wenn Sie die Bereitstellung in Ihrem IdP konfigurieren.

    a. SCIM-Endpunkt — Zum Beispiel https://scim. *us-east-2*.amazonaws.com/ /scim/v2 *11111111111-2222-3333-4444-555555555555*

    b. Zugriffstoken — Wählen Sie Token anzeigen, um den Wert zu kopieren.

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

werden diese Werte eingeben, um die automatische Bereitstellung in Ihrem IdP später in diesem Tutorial zu konfigurieren.

5. Klicken Sie auf Close (Schließen).

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

Schritt 2: Konfigurieren Sie die Bereitstellung in JumpCloud

Verwenden Sie das folgende Verfahren in der JumpCloud IAM Identity Center-Connector, um die Bereitstellung mit IAM Identity Center zu ermöglichen. Bei diesem Verfahren wird davon ausgegangen, dass Sie das bereits hinzugefügt haben JumpCloud IAM Identity Center-Connector zu Ihrem JumpCloud Admin-Portal und Gruppen. Falls Sie dies noch nicht getan haben, finden Sie weitere Informationen unter diesem Verfahren zur Voraussetzungen Konfiguration der SCIM-Bereitstellung und führen Sie es anschließend aus.

So konfigurieren Sie die Bereitstellung in JumpCloud

1. Öffnen Sie JumpCloud IAM Identity Center-Connector, 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-Connector und dann die dritte Registerkarte Identity Management.
3. Aktivieren Sie das Kontrollkästchen Verwaltung von Benutzergruppen und Gruppenmitgliedschaften in dieser Anwendung aktivieren, wenn Sie möchten, dass Gruppen mit SCIM synchronisiert werden.
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.
6. Aus dem vorherigen Verfahren haben Sie den Wert des Zugriffstokens in IAM Identity Center kopiert. Fügen Sie diesen Wert in das Feld Token-Schlüssel im JumpCloud IAM Identity Center-Konnektor.
7. Klicken Sie auf Aktivieren, um die Konfiguration zu übernehmen.
8. Vergewissern Sie sich, dass neben Single Sign-On aktiviert eine grüne Anzeige angezeigt wird.

9. Gehen Sie zur vierten Registerkarte Benutzergruppen und markieren Sie die Gruppen, für die Sie SCIM bereitstellen möchten.
10. Wenn Sie fertig sind, klicken Sie unten auf Speichern.
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 erscheinen auf der Benutzerseite. Diese Benutzer können jetzt Konten in IAM Identity Center zugewiesen werden.

(Optional) Schritt 3: Konfigurieren Sie Benutzerattribute in JumpCloud für die Zugriffskontrolle im IAM Identity Center

Dies ist ein optionales Verfahren für JumpCloud sollten Sie sich dafür entscheiden, Attribute für IAM Identity Center zu konfigurieren, um den Zugriff auf Ihre AWS Ressourcen zu verwalten. Die Attribute, die Sie definieren in JumpCloud werden in einer SAML-Assertion an IAM Identity Center übergeben. Anschließend erstellen Sie in IAM Identity Center einen Berechtigungssatz, um den Zugriff auf der Grundlage der Attribute zu verwalten, von denen Sie übergeben haben JumpCloud.

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 im IAM Identity Center

1. Öffnen Sie JumpCloud IAM Identity Center-Connector, den Sie im Rahmen der Konfiguration von SAML für installiert haben JumpCloud (Benutzerauthentifizierung > IAM Identity Center).
2. Wählen Sie den IAM Identity Center-Connector. Wählen Sie dann die zweite Registerkarte IAM Identity Center.
3. Unten auf dieser Registerkarte befindet sich die Benutzerattribute-Zuordnung. Wählen Sie 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 möchten.

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

b. In der JumpCloud Wählen Sie im Feld „Attributname“ Benutzerattribute aus JumpCloud Verzeichnis. Zum Beispiel E-Mail (Arbeit).

4. Wählen Sie Save (Speichern) aus.

(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.

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

AWS IAM Identity Center unterstützt 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. Weitere Informationen finden Sie unter Verwenden des SAML- und SCIM-Identitätsverbunds mit externen Identitätsanbietern.

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 in der Microsoft Dokumentation unter Schnellstart: Einen Mandanten einrichten.
- Ein AWS IAM Identity Center-aktiviertes Konto. Weitere Informationen finden Sie unter Aktivieren von IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.

Überlegungen

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.

Automatische Bereitstellung

Bevor Sie mit der Bereitstellung von SCIM beginnen, empfehlen wir Ihnen, dies zunächst zu überprüfen. 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 Alternativ können Sie die konfigurierbare AD-Synchronisierung von IAM Identity Center verwenden, um Active Directory Gruppen in IAM Identity Center zu integrieren.

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 Dokumentation unter Einschränkungen der Vorschauversion.

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 den Ergebnissen 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 Sie im Feld Anzeigename den Wert ein **NikkiWolf**.
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 du dazu aufgefordert wirst, gib Nikkis Passwort ein und wähle 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 im linken Navigationsbereich 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 Zugriffsberechtigungen (über einen Berechtigungssatz) konfigurieren, manuell einen entsprechenden Nikki Wolf-Benutzer erstellen und ihr die erforderlichen Berechtigungen für die Verwaltung von Ressourcen in zuweisen. IAM Identity Center 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-Managementkonsole Alle anderen Berechtigungen zum Anzeigen oder Verwalten anderer Informationen für Nikkis Konto sind standardmäßig verweigert.

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wähle 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 aus.
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 aus, wählen Sie Benutzer hinzufügen und geben Sie dann die folgenden Informationen ein:
    a. Sowohl für den Benutzernamen als auch für die E-Mail-Adresse — Geben Sie dasselbe **`NikkiWolf`**@ ein*`yourcompanydomain.extension`*, das Sie bei der Erstellung Ihres Microsoft Entra ID Benutzers verwendet haben. Zum Beispiel NikkiWolf@*`example.org`*.
    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 anschließend „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. Markiere das Kästchen 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.
5. Example

   <caption>On the Wähle Berechtigungssätze aus page, choose the `RegionalAdmin` permission set created in Step 2.1, and then choose Next.</caption>
6. Überprüfen Sie auf der Seite Überprüfen und abschicken Ihre Auswahl und wählen Sie dann Senden 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 die XML-Datei 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 2 aus. Richten Sie Single Sign-On ein.
3. Wählen Sie auf der Seite Single Sign-On mit SAML einrichten die Option SAML aus. Wählen Sie dann Metadatendatei hochladen, 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. Vergewissern Sie sich auf der Seite Basic SAML Configuration, dass sowohl der Identifier - als auch der Antwort-URL-Wert jetzt auf Endpunkte verweisen AWS , die mit beginnen. `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 testen AWS IAM Identity Center, wählen Sie Nein, ich werde es später testen. 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 aus.
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 du dazu aufgefordert wirst, gib Nikkis Passwort ein und wähle dann Anmelden.
3. Wählen Sie auf der Seite Mein Konto im linken Navigationsbereich 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 Ihr AWS-Konten Display angezeigt wird.

   > **Tip**
   >
   > Wenn die Seite leer ist und keine AWS-Konten Anzeige angezeigt wird, vergewissern Sie sich, dass Nikki dem RegionalAdminBerechtigungssatz erfolgreich zugewiesen wurde (siehe **`Step 2.3`**).

Step 3.5

Schritt 3.5: Testen Sie Nikkis Zugriffsrechte, 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 die Registerkarte Konten, um die Liste der Konten anzuzeigen. Die Kontonamen IDs, Konten und E-Mail-Adressen aller Konten, für die Sie Berechtigungssätze definiert haben, werden angezeigt.

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-Managementkonsole 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 AWS Regionen. 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 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 Sie im Feld Anzeigename den Wert ein **`RichRoe`**.
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/ /scim/v2 *11111111111-2222-3333-4444-555555555555*

   b. Zugriffstoken — Wählen Sie Token anzeigen, um den Wert zu kopieren.

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

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 4.2`** 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.
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 Benutzerseite 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.

Schritt 5: ABAC konfigurieren — optional

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.

Configure user attributes in Microsoft Entra ID for access control in IAM Identity Center

Konfigurieren Sie Benutzerattribute Microsoft Entra ID für die Zugriffskontrolle im 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 Erstellen Sie einen Berechtigungssatz 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. 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. 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.

Configure ABAC using IAM Identity Center

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 `Department=billing` für das Tag zu übergeben:

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

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

Weisen Sie Zugriff zu AWS-Konten

Die folgenden Schritte sind nur erforderlich, um AWS-Konten nur Zugriff zu gewähren. Diese Schritte sind nicht erforderlich, um Zugriff auf AWS Anwendungen zu gewähren.

> **Note**
>
> Um diesen Schritt abzuschließen, benötigen Sie eine Organisationsinstanz von IAM Identity Center. Weitere Informationen finden Sie unter Organisations- und Kontoinstanzen von IAM Identity Center.

Schritt 1: IAM Identity Center: Gewähren Sie Microsoft Entra ID 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 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.

   iii. Stellen Sie für Schritt 3: Überprüfen und erstellen sicher, dass der Typ Berechtigungssatz die AWS verwaltete Richtlinie verwendet AdministratorAccess. Wählen Sie Erstellen aus. 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`*

Schritt 2Microsoft Entra ID: Bestätigen Sie den Zugriff der Microsoft Entra ID Benutzer auf AWS Ressourcen

1. Kehren Sie zur Microsoft Entra IDKonsole zurück und navigieren Sie zu Ihrer SAML-basierten Anmeldeanwendung für IAM Identity Center.
2. Wählen Sie Benutzer und Gruppen und anschließend Benutzer oder Gruppen hinzufügen aus. Sie fügen den Benutzer, den Sie in diesem Tutorial in Schritt 4 erstellt haben, der Microsoft Entra ID Anwendung hinzu. Indem Sie den Benutzer hinzufügen, ermöglichen Sie ihm, sich anzumelden AWS. Suchen Sie nach dem Benutzer, den Sie in Schritt 4 erstellt haben. Wenn Sie diesen Schritt befolgen würden, wäre das der Fall**`RichardRoe`**.

    - Eine Demo finden Sie unter Verbinden Sie Ihre bestehende IAM Identity Center-Instanz mit Microsoft Entra ID

Fehlerbehebung

Informationen zur allgemeinen SCIM- und SAML-Fehlerbehebung mit finden Sie in den folgenden Microsoft Entra ID Abschnitten:

- Synchronisierungsprobleme mit Microsoft Entra ID und IAM Identity Center
- Bestimmte Benutzer können sich von einem externen SCIM-Anbieter nicht mit dem IAM Identity Center synchronisieren
- Probleme mit dem Inhalt von SAML-Assertionen, die von IAM Identity Center erstellt wurden
- Beim Bereitstellen von Benutzern oder Gruppen mit einem externen Identitätsanbieter ist ein Fehler beim Duplizieren von Benutzern oder Gruppen aufgetreten
- Weitere Ressourcen

Synchronisierungsprobleme mit Microsoft Entra ID und IAM Identity Center

Wenn Sie Probleme mit Microsoft Entra ID Benutzern haben, die nicht mit IAM Identity Center synchronisieren, kann dies an einem Syntaxproblem liegen, 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 im CloudTrail Ereignis 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 Microsoft Entra ID und sicherzustellen, 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 Problembehandlung.

Microsoft Entra IDSynchronisation des Gastkontos

Wenn Sie Ihre Microsoft Entra ID Gastbenutzer mit IAM Identity Center synchronisieren möchten, gehen Sie wie folgt vor.

Microsoft Entra IDDie E-Mail-Adresse von Gastbenutzern unterscheidet sich von der E-Mail-Adresse von Microsoft Entra ID Benutzern. Dieser Unterschied führt zu Problemen beim Versuch, Microsoft Entra ID Gastbenutzer mit IAM Identity Center zu synchronisieren. Sehen Sie sich zum Beispiel die folgende E-Mail-Adresse für einen Gastbenutzer an:

`exampleuser_domain.com#EXT#@domain.onmicrosoft.com.`

IAM Identity Center geht nicht davon aus, dass die E-Mail-Adresse das *`#EXT#@domain`* Format enthält.

1. Melden Sie sich im Microsoft Entra Admin Center an und navigieren Sie zu Identität > Anwendungen > Unternehmensanwendungen und wählen Sie dann AWS IAM Identity Center
2. Navigieren Sie im linken Bereich zur Registerkarte Single Sign On.
3. Wählen Sie Bearbeiten aus, was neben Benutzerattribute und Ansprüche angezeigt wird.
4. Wählen Sie unter Erforderliche Ansprüche die Option Eindeutige Benutzerkennung (Name-ID) aus.
5. Sie werden zwei Anspruchsbedingungen für Ihre Microsoft Entra ID Benutzer und Gastbenutzer erstellen:

    a. Erstellen Sie für Microsoft Entra ID Benutzer einen Benutzertyp für Mitglieder, bei dem das Quellattribut auf gesetzt ist `user.userprincipalname`.

    b. Erstellen Sie für Microsoft Entra ID Gastbenutzer einen Benutzertyp für externe Gäste, wobei das Quellattribut auf gesetzt ist`user.mail`.

    c. Wählen Sie Speichern und versuchen Sie erneut, sich als Microsoft Entra ID Gastbenutzer anzumelden.

Weitere Ressourcen

- Allgemeine Tipps zur SCIM-Fehlerbehebung finden Sie unter. Behebung von Problemen mit IAM Identity Center
- Informationen zur Microsoft Entra ID Fehlerbehebung finden Sie in der MicrosoftDokumentation.
- Weitere Informationen zum Verbund zwischen mehreren AWS-Konten finden Sie unter Sichern AWS-Konten mit Azure Active Directory Federation.

Die folgenden Ressourcen können Ihnen bei der Problembehebung bei der Arbeit mit helfen AWS:

- AWS re:Post- Hier finden Sie weitere Ressourcen FAQs und Links zu diesen, die Ihnen bei der Behebung von Problemen helfen.
- AWS Support- Holen Sie sich technischen Support

Konfiguration von SAML und SCIM mit einem IAM Okta Identity Center

Mithilfe des SCIM 2.0-Protokolls (System for Cross-Domain Identity Management) Okta können Sie Benutzer- und Gruppeninformationen automatisch aus dem IAM Identity Center bereitstellen oder synchronisieren. Weitere Informationen finden Sie unter Verwenden des SAML- und SCIM-Identitätsverbunds mit externen Identitätsanbietern.

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 Ihrem Konto. 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.

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 Lifecycle-Management oder ähnliche Funktionen unterstützt, die eine ausgehende Bereitstellung ermöglichen. Diese Funktionen sind möglicherweise erforderlich, um SCIM von zu IAM Identity Center Okta zu konfigurieren.
> Wenn Sie IAM Identity Center noch nicht aktiviert haben, finden Sie weitere Informationen unter. IAM Identity Center aktivieren

Überlegungen

- 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
- 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, die mehrere Werte haben, 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.
- Bei Verwendung Okta mit IAM Identity Center wird IAM Identity Center in der Regel als Anwendung in konfiguriert. Okta Auf diese Weise können Sie mehrere Instanzen von IAM Identity Center als mehrere Anwendungen konfigurieren, die den Zugriff auf mehrere AWS Organizations innerhalb einer einzigen Instanz von unterstützen. Okta

- Berechtigungen und Rollenattribute werden nicht unterstützt und können nicht mit IAM Identity Center synchronisiert werden.
- Die Verwendung derselben Okta Gruppe sowohl für Zuweisungen als auch für 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 1Okta: 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: IAM Identity Center: 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-Metadaten 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“.

   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. Wählen Sie dann Bearbeiten aus.

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 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: IAM Identity Center undOkta: Benutzer bereitstellen 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:

   a. SCIM-Endpunkt — Zum Beispiel https://scim. *us-east-2*.amazonaws.com/ /scim/v2 *11111111111-2222-3333-4444-555555555555*

   b. Zugriffstoken — Wählen Sie Token anzeigen, um den Wert zu kopieren.

   > **Warning**
   >
   > Dies ist das einzige Mal, dass Sie den SCIM-Endpunkt und das Zugriffstoken abrufen können. Stellen Sie sicher, dass Sie diese Werte kopieren, bevor Sie fortfahren. Sie werden diese Werte Okta später in diesem Tutorial eingeben, um die automatische Bereitstellung zu konfigurieren.

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 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 automatische Bereitstellung zu aktivieren.
7. Verwenden Sie für die Konfiguration Okta die SCIM-Bereitstellungswerte AWS IAM Identity Center , die Sie zuvor in diesem Schritt kopiert haben:

a. Geben Sie im Feld Basis-URL den SCIM-Endpunktwert ein.

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 in den Bereich Einstellungen verschoben, 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 4Okta: 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 AWS 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. So weisen Sie Gruppen zu:

- Wählen Sie auf der Seite „Zuweisungen“ die Option „Zuweisen“ und dann „Zu 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 Sie mit IAM Identity Center synchronisieren möchten. Wählen Sie Speichern.

   Der Gruppenstatus ändert sich in Aktiv, nachdem die Gruppe und ihre Mitglieder per Push an IAM Identity Center weitergeleitet wurden.
3. Kehren Sie zur Registerkarte „Zuweisungen“ zurück.
4. Gehen Sie wie folgt vor, um einzelne Okta Benutzer zu IAM Identity Center hinzuzufügen:

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

   b. 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.

5. 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.

Übergabe von Attributen für die Zugriffskontrolle — optional

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.

Weisen Sie Zugriff zu AWS-Konten

Die folgenden Schritte sind nur erforderlich, um AWS-Konten nur Zugriff zu gewähren. Diese Schritte sind nicht erforderlich, um Zugriff auf AWS Anwendungen zu gewähren.

> **Note**
>
> Um diesen Schritt abzuschließen, benötigen Sie eine Organisationsinstanz von IAM Identity Center. Weitere Informationen finden Sie unter Organisations- und Kontoinstanzen von IAM Identity Center.

Schritt 1: IAM Identity Center: Gewähren Sie Okta Benutzern Zugriff auf Konten

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 beim Erstellen 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 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.

iii. Stellen Sie für Schritt 3: Überprüfen und erstellen sicher, dass der Typ Berechtigungssatz die AWS verwaltete Richtlinie verwendet AdministratorAccess. Wählen Sie Erstellen aus. 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*

Schritt 2Okta: Bestätigen Sie den Okta Benutzerzugriff auf Ressourcen AWS

1. Melden Sie sich mit einem Testkonto bei der anOkta dashboard.
2. Wählen Sie unter Meine Apps das AWS IAM Identity Center Symbol aus.
3. Sie sollten das AWS-Konto Symbol sehen. Erweitern Sie dieses Symbol, um die Liste zu sehen, auf AWS-Konten 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 sowohl den Zugriff auf den als auch den AWS-Managementkonsole programmatischen Zugriff angegeben. Wählen Sie Managementkonsole aus, um die zu öffnen. AWS-Managementkonsole
6. Der Benutzer ist bei angemeldet AWS-Managementkonsole.

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 Benutzer- oder Gruppenzugriff 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.

Fehlerbehebung

Informationen zur allgemeinen SCIM- und SAML-Problembehandlung mit Okta finden Sie in den folgenden Abschnitten:

- Erneute Bereitstellung von Benutzern und Gruppen, die aus IAM Identity Center gelöscht wurden
- Fehler bei der automatischen Bereitstellung in Okta
- Bestimmte Benutzer können sich von einem externen SCIM-Anbieter nicht mit dem IAM Identity Center synchronisieren
- Probleme mit dem Inhalt von SAML-Assertionen, die von IAM Identity Center erstellt wurden
- Beim Bereitstellen von Benutzern oder Gruppen mit einem externen Identitätsanbieter ist ein Fehler beim Duplizieren von Benutzern oder Gruppen aufgetreten
- Weitere Ressourcen

Erneute Bereitstellung von Benutzern und Gruppen, die aus IAM Identity Center gelöscht wurden

- Wenn Sie versuchen, einen Benutzer oder eine Gruppe zu ändern, die einmal synchronisiert und dann aus IAM Identity Center gelöscht wurdeOkta, wird möglicherweise die folgende Fehlermeldung in der Okta Konsole angezeigt:
  - Der automatische Profil-Push des Benutzers *`Jane Doe`* zur App ist AWS IAM Identity Center fehlgeschlagen: Fehler beim Versuch, die Profilaktualisierung für zu pushen*`jane_doe@example.com`*: Für den Benutzer wurde kein Benutzer zurückgegeben *`xxxxx-xxxxxx-xxxxx-xxxxxxx`*
  - Die verknüpfte Gruppe fehlt in AWS IAM Identity Center. Ändern Sie die verknüpfte Gruppe, um weiterhin Gruppenmitgliedschaften zu übertragen.
- Möglicherweise erhalten Sie auch die folgende Fehlermeldung in den Okta Systemprotokollen für synchronisierte und gelöschte IAM Identity Center-Benutzer oder -Gruppen:
  - Okta-Fehler: Eventfailed application.provision.user.push_profile: Für den Benutzer wurde kein Benutzer zurückgegeben *`xxxxx-xxxxxx-xxxxx-xxxxxxx`*
  - Okta-Fehler: application.provision.group_push.mapping.update.or.delete.failed.with.error: Die verknüpfte Gruppe fehlt in. AWS IAM Identity CenterÄndern Sie die verknüpfte Gruppe, um weiterhin Gruppenmitgliedschaften zu übertragen.

> **Warning**
>
> Benutzer und Gruppen sollten Okta nicht aus dem IAM Identity Center gelöscht werden, wenn Sie das IAM Identity Center mit SCIM synchronisiert Okta haben.

Fehlerbehebung für gelöschte IAM Identity Center-Benutzer

Um dieses Problem mit gelöschten IAM Identity Center-Benutzern zu beheben, müssen die Benutzer von gelöscht werden. Okta Falls erforderlich, müssten diese Benutzer auch in neu erstellt werden. Okta Wenn der Benutzer neu erstellt wirdOkta, wird er ebenfalls über SCIM erneut im IAM Identity Center bereitgestellt. Weitere Informationen zum Löschen eines Benutzers finden Sie in der Dokumentation. Okta

> **Note**
>
> Wenn Sie einem Okta Benutzer den Zugriff auf IAM Identity Center entziehen müssen, sollten Sie ihn zuerst aus seinem Gruppen-Push und dann aus seiner Zuweisungsgruppe entfernen. Okta Dadurch wird sichergestellt, dass der Benutzer aus der ihm zugewiesenen Gruppenmitgliedschaft in IAM Identity Center entfernt wird. Weitere Informationen zur Fehlerbehebung bei Group Push finden Sie in der OktaDokumentation.

Fehlerbehebung bei gelöschten IAM Identity Center-Gruppen

Um dieses Problem mit gelöschten IAM Identity Center-Gruppen zu beheben, muss die Gruppe aus Okta gelöscht werden. Falls erforderlich, müssten diese Gruppen auch in Okta mithilfe von Group Push neu erstellt werden. Wenn der Benutzer in Okta neu erstellt wird, wird er auch über SCIM erneut im IAM Identity Center bereitgestellt. Weitere Informationen zum Löschen einer Gruppe finden Sie in der Okta-Dokumentation.

Fehler bei der automatischen Bereitstellung in Okta

Wenn Sie die folgende Fehlermeldung erhalten inOkta:

Die automatische Bereitstellung des Benutzers Jane Doe für die App ist AWS IAM Identity Center fehlgeschlagen: Der passende Benutzer wurde nicht gefunden

Weitere Informationen finden Sie in der OktaDokumentation.

Weitere Ressourcen

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

Die folgenden Ressourcen können Ihnen bei der Problembehebung bei der Arbeit mit AWS helfen:

- AWS re:Post- Hier finden Sie weitere Ressourcen FAQs und Links zu diesen, die Ihnen bei der Behebung von Problemen helfen.
- AWS Support- Holen Sie sich technischen Support

Einrichtung der SCIM-Bereitstellung zwischen OneLogin und IAM Identity Center

IAM Identity Center unterstützt die automatische Bereitstellung (Synchronisation) von Benutzer- und Gruppeninformationen von OneLogin über das SCIM v2.0-Protokoll (System for Cross-Domain Identity Management) in das IAM Identity Center. Weitere Informationen finden Sie unter Verwenden des SAML- und SCIM-Identitätsverbunds mit externen Identitätsanbietern.

Sie konfigurieren diese Verbindung in OneLogin, indem Sie Ihren SCIM-Endpunkt für IAM Identity Center und ein Bearer-Token verwenden, 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. Dadurch stimmen die erwarteten Attribute zwischen IAM Identity Center und OneLogin.

In den folgenden Schritten erfahren Sie, wie Sie die automatische Bereitstellung von Benutzern und Gruppen von aktivieren OneLogin über das SCIM-Protokoll zu IAM Identity Center.

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

Themen

Voraussetzungen

Bevor Sie beginnen können, benötigen Sie Folgendes:

- A OneLogin Konto. Wenn Sie noch kein Konto haben, können Sie möglicherweise ein kostenloses Test- oder Entwicklerkonto bei der OneLogin Webseite.
- Ein IAM Identity Center-fähiges Konto (kostenlos). Weitere Informationen finden Sie unter IAM Identity Center aktivieren.
- Eine SAML-Verbindung von Ihrem OneLogin Konto für IAM Identity Center. Weitere Informationen finden Sie unter Aktivieren von Single Sign-On zwischen OneLogin und AWS im AWS Partner Network-Blog.

Schritt 1: Aktivieren Sie die Bereitstellung im IAM Identity Center

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

Um die automatische Bereitstellung in 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 den SCIM-Endpunkt und das Zugriffstoken. Sie müssen diese später einfügen, wenn Sie die Bereitstellung in Ihrem IdP konfigurieren.

   a. SCIM-Endpunkt — Zum Beispiel https://scim. *us-east-2*.amazonaws.com/ /scim/v2 *1111111111-2222-3333-4444-555555555555*

   b. Zugriffstoken — Wählen Sie Token anzeigen, um den Wert zu kopieren.

> **Warning**
>
> Dies ist das einzige Mal, dass Sie den SCIM-Endpunkt und das Zugriffstoken abrufen können. Stellen Sie sicher, dass Sie diese Werte kopieren, bevor Sie fortfahren. Sie werden diese Werte eingeben, um die automatische Bereitstellung in Ihrem IdP später in diesem Tutorial zu konfigurieren.

5. Klicken Sie auf Close (Schließen).

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

Schritt 2: Konfigurieren Sie die Bereitstellung in OneLogin

Verwenden Sie das folgende Verfahren in der OneLogin Admin-Konsole, um die Integration zwischen IAM Identity Center und der IAM Identity Center-App zu ermöglichen. Bei diesem Verfahren wird davon ausgegangen, dass Sie die AWS Single Sign-On-Anwendung bereits konfiguriert haben OneLogin für die SAML-Authentifizierung. Wenn Sie diese SAML-Verbindung noch nicht hergestellt haben, tun Sie dies, bevor Sie fortfahren, und kehren Sie dann hierher zurück, um den SCIM-Bereitstellungsprozess abzuschließen. Weitere Informationen zur Konfiguration von SAML mit OneLogin, siehe Single Sign-On aktivieren zwischen OneLogin und AWS im AWS Partner Network-Blog.

Um die Bereitstellung zu konfigurieren in OneLogin

1. Melden Sie sich an bei OneLogin, und 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 sie aus und wählen Sie dann im Navigationsbereich 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 ein OneLogin. Außerdem haben Sie im vorherigen Verfahren den Wert des Zugriffstokens in IAM Identity Center kopiert. Fügen Sie diesen Wert in das Feld SCIM-Bearer-Token ein OneLogin.
4. Klicken Sie neben API-Verbindung auf Aktivieren und dann auf Speichern, um die Konfiguration abzuschließen.
5. Wählen Sie im Navigationsbereich Provisioning (Bereitstellung) aus.
6. Aktivieren Sie die Kontrollkästchen für Bereitstellung aktivieren, Benutzer erstellen, Benutzer löschen und Benutzer aktualisieren und wählen Sie dann Speichern aus.
7. Klicken Sie im Navigationsbereich auf Users (Benutzer).
8. Klicken Sie auf Weitere Aktionen und wählen Sie Logins synchronisieren aus. Sie sollten die Meldung Benutzer mit AWS Single Sign-On synchronisieren erhalten.

9. Klicken Sie erneut auf Weitere Aktionen und wählen Sie dann Berechtigungszuordnungen erneut anwenden aus. Sie sollten die Meldung „Zuordnungen 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 Event-Stream erscheinen.
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 erscheinen auf der Benutzerseite. Sie können Ihre synchronisierten Gruppen auch auf der Gruppenseite 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 Sie Benutzerattribute in OneLogin für die Zugriffskontrolle im IAM Identity Center

Dies ist ein optionales Verfahren für OneLogin wenn Sie sich dafür entscheiden, Attribute zu konfigurieren, die Sie in IAM Identity Center verwenden werden, um den Zugriff auf Ihre AWS Ressourcen zu verwalten. Die Attribute, die Sie definieren in OneLogin werden in einer SAML-Assertion an IAM Identity Center übergeben. Anschließend erstellen Sie in IAM Identity Center einen Berechtigungssatz, um den Zugriff auf der Grundlage der Attribute zu verwalten, von denen Sie die Daten übergeben haben OneLogin.

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.

Um Benutzerattribute zu konfigurieren in OneLogin für die Zugriffskontrolle im IAM Identity Center

1. Melden Sie sich an bei OneLogin, und 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 sie aus und wählen Sie dann im Navigationsbereich die Option 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 +.

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

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

d. Verwenden Sie im Feld Wert die Dropdownliste, um Folgendes auszuwählen OneLogin Benutzerattribute. Zum Beispiel Abteilung.

4. Wählen Sie Save (Speichern) aus.

(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.

Fehlerbehebung

Im Folgenden können Sie einige häufig auftretende Probleme beheben, die bei der Einrichtung der automatischen Bereitstellung auftreten können OneLogin.

Gruppen werden nicht für IAM Identity Center bereitgestellt

Standardmäßig können Gruppen nicht von bereitgestellt werden OneLogin zum IAM Identity Center. Stellen Sie sicher, dass Sie die Gruppenbereitstellung für Ihre IAM Identity Center-Anwendung aktiviert haben in OneLogin. Melden Sie sich dazu bei OneLogin Admin-Konsole und stellen Sie sicher, dass in den Eigenschaften der IAM Identity Center-Anwendung (IAM Identity Center-Anwendung > Parameter > Gruppen) die Option In die Benutzerbereitstellung einbeziehen ausgewählt ist. Weitere Informationen zum Erstellen von Gruppen finden Sie in OneLogin, einschließlich der Vorgehensweise beim Synchronisieren OneLogin Rollen als Gruppen in SCIM finden Sie im OneLogin Webseite.

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

Zusätzlich zu dem obigen Hinweis zur Genehmigung durch den Administrator 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 finden Sie unter OneLogin, einschließlich Synchronisierungsereignissen, unter Aktivität > Ereignisse.

Ich habe eine Gruppe gelöscht oder deaktiviert in OneLogin, aber sie wird immer noch im IAM Identity Center angezeigt

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

Ich habe eine Gruppe in IAM Identity Center gelöscht, ohne sie vorher 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 Regeln oder Konfigurationen für die Gruppenbereitstellung in OneLogin. Zum Beispiel eine Gruppe, die einer Anwendung direkt zugewiesen ist, zusammen mit einer Regel, die in derselben Gruppe veröffentlicht. Löschen Sie anschließend alle unerwünschten Gruppen in IAM Identity Center. Endlich in OneLogin, Aktualisieren Sie die Berechtigungen (IAM Identity Center App > Provisioning > Berechtigungen) und wenden Sie dann die Berechtigungszuordnungen erneut an (IAM Identity Center App > Weitere Aktionen). Um dieses Problem in future zu vermeiden, nehmen Sie zunächst die Änderung vor, um die Bereitstellung der Gruppe in zu beenden OneLoginund löschen Sie dann die Gruppe aus IAM Identity Center.

Die Verwendung von Ping Identity Produkte mit IAM Identity Center

Folgendes Ping Identity Produkte wurden mit IAM Identity Center getestet.

Themen

PingFederate

IAM Identity Center unterstützt die automatische Bereitstellung (Synchronisation) von Benutzer- und Gruppeninformationen aus PingFederate Produkt von Ping Identity (im Folgenden“Ping“) in das IAM Identity Center. Bei dieser Bereitstellung wird das SCIM-Protokoll (System for Cross-Domain Identity Management) v2.0 verwendet. Weitere Informationen finden Sie unter Verwenden des SAML- und SCIM-Identitätsverbunds mit externen Identitätsanbietern.

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. Dadurch stimmen die erwarteten Attribute zwischen IAM Identity Center und PingFederate.

Dieser Leitfaden basiert auf PingFederate Version 10.2. Die Schritte für andere Versionen können variieren. Kontakt Ping für weitere Informationen zur Konfiguration der Bereitstellung im IAM Identity Center für andere Versionen von PingFederate.

In den folgenden Schritten erfahren Sie, wie Sie die automatische Bereitstellung von Benutzern und Gruppen von aktivieren PingFederate über das SCIM-Protokoll zu IAM Identity Center.

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

Themen

- Schritt 1: Aktivieren Sie die Bereitstellung im IAM Identity Center
- Schritt 2: Konfigurieren Sie die Bereitstellung in PingFederate
- (Optional) Schritt 3: Konfigurieren Sie Benutzerattribute in PingFedFür die Zugriffskontrolle im IAM Identity Center erstellen
- (Optional) Übergabe von Attributen für die Zugriffskontrolle
- Fehlerbehebung

Voraussetzungen

Bevor Sie beginnen können, benötigen Sie Folgendes:

- Ein funktionierendes PingFederate Server. Wenn Sie noch keinen vorhandenen haben PingFederate Server, möglicherweise können Sie auf der Ping Identity-Website ein kostenloses Test- oder Entwicklerkonto beantragen. Die Testversion umfasst Lizenzen und Software-Downloads sowie die zugehörige Dokumentation.
- Eine Kopie der PingFederate Die IAM Identity Center Connector-Software ist auf Ihrem installiert PingFederate Server. Weitere Informationen darüber, wie Sie diese Software erhalten, 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 Ihrem PingFederate Instanz zum IAM Identity Center. Anweisungen zur Konfiguration dieser Verbindung finden Sie im PingFederate -Dokumentation. Zusammenfassend lässt sich sagen, dass der empfohlene Weg darin besteht, den IAM Identity Center Connector zur Konfiguration von „Browser SSO“ in zu verwenden PingFederate, wobei die Funktionen „Herunterladen“ und „Importieren“ von Metadaten an beiden Enden verwendet werden, um SAML-Metadaten zwischen PingFederate und IAM Identity Center.

Überlegungen

Im Folgenden finden Sie wichtige Überlegungen zu PingFederate das kann sich darauf auswirken, wie Sie die Bereitstellung mit IAM Identity Center implementieren.

- Wenn ein Attribut (z. B. eine Telefonnummer) von einem Benutzer im Datenspeicher entfernt wird, der in konfiguriert ist PingFederate, wird dieses Attribut nicht von dem entsprechenden Benutzer in IAM Identity Center entfernt. Dies ist eine bekannte Einschränkung in PingFederate’s

Implementierung des Provisioners. Wenn ein Attribut für einen Benutzer in einen anderen (nicht leeren) Wert geändert wird, wird diese Änderung mit IAM Identity Center synchronisiert.

Schritt 1: Aktivieren Sie die Bereitstellung im IAM Identity Center

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

Um die automatische Bereitstellung in 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 den SCIM-Endpunkt und das Zugriffstoken. Sie müssen diese später einfügen, wenn Sie die Bereitstellung in Ihrem IdP konfigurieren.

   a. SCIM-Endpunkt — Zum Beispiel https://scim. *us-east-2*.amazonaws.com/ /scim/v2 *11111111111-2222-3333-4444-555555555555*

   b. Zugriffstoken — Wählen Sie Token anzeigen, um den Wert zu kopieren.

   > **Warning**
   >
   > Dies ist das einzige Mal, dass Sie den SCIM-Endpunkt und das Zugriffstoken abrufen können. Stellen Sie sicher, dass Sie diese Werte kopieren, bevor Sie fortfahren. Sie werden diese Werte eingeben, um die automatische Bereitstellung in Ihrem IdP später in diesem Tutorial zu konfigurieren.

5. Klicken Sie auf Close (Schließen).

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

Schritt 2: Konfigurieren Sie die Bereitstellung in PingFederate

Verwenden Sie das folgende Verfahren in der PingFederate Verwaltungskonsole, um die Integration zwischen IAM Identity Center und dem IAM Identity Center Connector zu ermöglichen. Bei diesem Verfahren wird davon ausgegangen, dass Sie die IAM Identity Center Connector-Software bereits installiert haben. Falls Sie dies noch nicht getan haben, finden Sie weitere Informationen zur Voraussetzungen Konfiguration der SCIM-Bereitstellung in diesem Verfahren und führen Sie es anschließend aus.

> **Important**
>
> Wenn Ihre PingFederate Der Server wurde noch nicht für die ausgehende SCIM-Bereitstellung konfiguriert. Möglicherweise müssen Sie eine Änderung der Konfigurationsdatei vornehmen, um die Bereitstellung zu aktivieren. Weitere Informationen finden Sie unter Ping -Dokumentation. Zusammenfassend müssen Sie die Einstellung in der `pf.provisioner.mode` pingfederate-<version>/pingfederate/bin/run.propertiessetzen Sie die Datei auf einen anderen Wert als `OFF` (was die Standardeinstellung ist) und starten Sie den Server neu, falls er gerade läuft. Sie können beispielsweise Folgendes verwenden, `STANDALONE` wenn Sie derzeit keine Hochverfügbarkeitskonfiguration haben PingFederate.

Um die Bereitstellung zu konfigurieren in PingFederate

1. Melden Sie sich an bei PingFederate Administrationskonsole.
2. Wählen Sie oben auf der Seite Anwendungen aus und klicken Sie dann auf SP-Verbindungen.
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 dunklen Navigationsüberschriften oben auf der Seite den Verbindungstyp aus. Sie sollten sehen, dass Browser-SSO bereits aus Ihrer vorherigen SAML-Konfiguration ausgewählt wurde. Wenn nicht, müssen Sie zuerst diese Schritte 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 Speichern. 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.
6. Klicken Sie wiederholt auf Weiter, bis Sie zur Seite Outbound Provisioning gelangen, und klicken Sie dann auf die Schaltfläche Provisioning konfigurieren.

7. Im vorherigen Verfahren haben Sie den SCIM-Endpunktwert in IAM Identity Center kopiert. Fügen Sie diesen Wert in das SCIM-URL-Feld im PingFederate console. Außerdem haben Sie im vorherigen Verfahren den Wert des Zugriffstokens in IAM Identity Center kopiert. Fügen Sie diesen Wert in das Feld Zugriffstoken im PingFederate console. Klicken Sie auf Speichern.
8. Klicken Sie auf der Seite Kanalkonfiguration (Kanäle konfigurieren) auf Erstellen.
9. Geben Sie einen Kanalnamen für diesen neuen Provisioning-Kanal 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 zum IAM Identity Center verwenden möchten, und klicken Sie auf Weiter.

> **Note**
>
> Wenn Sie noch keine Datenquelle konfiguriert haben, müssen Sie dies jetzt tun. Sehen Sie sich die Ping In der Produktdokumentation finden Sie Informationen zur Auswahl und Konfiguration einer Datenquelle in PingFederate.

11. Vergewissern Sie sich auf der Seite mit den 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 existiert, 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) durchsucht werden sollen, und geben Sie alle erforderlichen LDAP-Filter an.

    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 dabei um denselben DN handeln, den Sie im Abschnitt Benutzer angegeben haben. Geben Sie nach Bedarf Werte für verschachtelte Suche und Filter ein.

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 formatiert ist (user@domain.com). Es muss auch dem Wert entsprechen, den der Benutzer für die Anmeldung bei Ping verwenden wird. Dieser Wert wird wiederum während der Verbundauthentifizierung in den `nameId` SAML-Anspruch übernommen und für den Abgleich mit dem Benutzer in IAM Identity Center verwendet. Wenn Sie beispielsweise Active Directory verwenden, können Sie den `UserPrincipalName` als UserName angeben.

b. Andere Felder mit dem Suffix * müssen Attributen zugeordnet werden, die für Ihre Benutzer ungleich Null sind.

14. Setzen Sie auf der Seite Aktivierung und Zusammenfassung den Kanalstatus auf Aktiv, 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. An diesem Punkt beginnt die Bereitstellung. Um die Aktivität zu bestätigen, können Sie sich die Datei provisioner.log ansehen, die sich standardmäßig im pingfederate-<version>/pingfederate/logVerzeichnis auf Ihrem PingFederate Server.
18. Um zu überprüfen, ob Benutzer und Gruppen erfolgreich mit IAM Identity Center synchronisiert wurden, kehren Sie zur IAM Identity Center Console zurück und wählen Sie Benutzer aus. Synchronisierte Benutzer von PingFederate erscheinen auf der Benutzerseite. Sie können synchronisierte Gruppen auch auf der Gruppenseite anzeigen.

(Optional) Schritt 3: Konfigurieren Sie Benutzerattribute in PingFedFür die Zugriffskontrolle im IAM Identity Center erstellen

Dies ist ein optionales Verfahren für PingFederate wenn Sie sich dafür entscheiden, Attribute zu konfigurieren, die Sie in IAM Identity Center verwenden werden, um den Zugriff auf Ihre AWS Ressourcen zu verwalten. Die Attribute, die Sie definieren in PingFederate werden in einer SAML-Assertion an IAM Identity Center übergeben. Anschließend erstellen Sie in IAM Identity Center einen Berechtigungssatz, um den Zugriff auf der Grundlage der Attribute zu verwalten, von denen Sie die Daten übergeben haben PingFederate.

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.

Um Benutzerattribute zu konfigurieren PingFederate für die Zugriffskontrolle im IAM Identity Center

1. Melden Sie sich an bei PingFederate Administrationskonsole.
2. Wählen Sie oben auf der Seite Anwendungen aus und klicken Sie dann auf SP-Verbindungen.
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 dunklen Navigationsüberschriften oben auf der Seite die Option Browser-SSO aus. Klicken Sie anschließend 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 „Assertionserstellung konfigurieren“ die Option Attributvertrag aus.
7. Fügen Sie auf der Seite „Attributvertrag“ im Abschnitt „Vertrag verlängern“ ein neues Attribut hinzu, indem Sie die folgenden Schritte ausführen:

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

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

   c. Wählen Sie „Hinzufügen“ und anschließend „Weiter“.
8. Wählen Sie auf der Seite „Zuordnung der Authentifizierungsquelle“ die mit Ihrer Anwendung konfigurierte Adapterinstanz aus.
9. Wählen Sie auf der Seite „Erfüllung des Attributvertrags“ die Quelle (Datenspeicher) und den Wert (Datenspeicherattribut) für den Attributvertrag aus`https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Department`**.

   > **Note**
   >
   > Wenn Sie noch keine Datenquelle konfiguriert haben, müssen Sie dies jetzt tun. Sehen Sie sich das an Ping In der Produktdokumentation finden Sie Informationen zur Auswahl und Konfiguration einer Datenquelle in PingFederate.
10. Klicken Sie wiederholt auf Weiter, bis Sie zur Seite Aktivierung und Zusammenfassung gelangen, und klicken Sie dann auf Speichern.

(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.

Fehlerbehebung

Für allgemeine SCIM- und SAML-Problembehebungen mit PingFederate, finden Sie in den folgenden Abschnitten:

- Bestimmte Benutzer können sich von einem externen SCIM-Anbieter nicht mit dem IAM Identity Center synchronisieren
- Probleme mit dem Inhalt von SAML-Assertionen, die von IAM Identity Center erstellt wurden
- Beim Bereitstellen von Benutzern oder Gruppen mit einem externen Identitätsanbieter ist ein Fehler beim Duplizieren von Benutzern oder Gruppen aufgetreten
- Weitere Informationen zu PingFederate, siehe PingFederate Dokumentation.

Die folgenden Ressourcen können Ihnen bei der Problembehebung bei der Arbeit mit helfen AWS:

- AWS re:Post- Hier finden Sie weitere Ressourcen FAQs und Links zu diesen, die Ihnen bei der Behebung von Problemen helfen.

- AWS Support- Holen Sie sich technischen Support

PingOne

IAM Identity Center unterstützt die automatische Bereitstellung (Synchronisation) von Benutzerinformationen aus PingOne Produkt von Ping Identity (im Folgenden“Ping“) in das IAM Identity Center. Bei dieser Bereitstellung wird das SCIM-Protokoll (System for Cross-Domain Identity Management) v2.0 verwendet. 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. Dadurch stimmen die erwarteten Attribute zwischen IAM Identity Center und PingOne.

In den folgenden Schritten erfahren Sie, wie Sie die automatische Bereitstellung von Benutzern von aktivieren PingOne über das SCIM-Protokoll zu IAM Identity Center.

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

Themen

Voraussetzungen

Bevor Sie beginnen können, benötigen Sie Folgendes:

- A PingOne Abonnement oder kostenlose Testversion mit föderierten Authentifizierungs- und Bereitstellungsfunktionen. Weitere Informationen darüber, wie Sie eine kostenlose Testversion erhalten können, finden Sie auf Ping IdentityWebsite.
- Ein IAM Identity Center-fähiges Konto (kostenlos). Weitere Informationen finden Sie unter IAM Identity Center aktivieren.
- Das Tool PingOne Die IAM Identity Center-Anwendung wurde zu Ihrem hinzugefügt PingOne Admin-Portal. Sie können das erhalten PingOne Die IAM Identity Center-Anwendung finden Sie unter PingOne Anwendungskatalog. Allgemeine Informationen finden Sie unter Hinzufügen einer Anwendung aus dem Anwendungskatalog auf der Ping Identity Website.
- Eine SAML-Verbindung von Ihrem PingOne Instanz zum IAM Identity Center. Nach dem PingOne Die IAM Identity Center-Anwendung wurde zu Ihrer hinzugefügt PingOne Admin-Portal, Sie müssen es verwenden, um eine SAML-Verbindung von Ihrem PingOne Instanz zum IAM Identity Center. Verwenden Sie die Funktionen „Metadaten herunterladen“ und „Importieren“ an beiden Enden, um SAML-Metadaten zwischen PingOne und IAM Identity Center. Anweisungen zur Konfiguration dieser Verbindung finden Sie im PingOne -Dokumentation.

Überlegungen

Im Folgenden finden Sie wichtige Überlegungen zu PingOne das kann sich darauf auswirken, wie Sie die Bereitstellung mit IAM Identity Center implementieren.

- PingOne unterstützt die Bereitstellung von Gruppen über SCIM nicht. Kontakt Ping für die neuesten Informationen zur Gruppenunterstützung in SCIM für PingOne.
- Benutzer können weiterhin Provisioning von erhalten PingOne nach der Deaktivierung der Bereitstellung in PingOne Admin-Portal. Wenn Sie die Bereitstellung sofort beenden müssen, löschen Sie das entsprechende SCIM-Bearer-Token und/oder deaktivieren Sie es Stellen Sie Benutzer und Gruppen von einem externen Identitätsanbieter mithilfe von SCIM bereit im IAM Identity Center.
- Wenn ein Attribut für einen Benutzer aus dem in konfigurierten Datenspeicher entfernt wird PingOne, wird dieses Attribut nicht aus dem entsprechenden Benutzer in IAM Identity Center entfernt. Dies ist eine bekannte Einschränkung in PingOne’s Implementierung des Provisioners. Wenn ein Attribut geändert wird, wird die Änderung mit dem 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 einzigartig ist PingOne,

ungleich Null und als E-Mail/UPN formatiert (z. B. user@domain.com) für Ihre SAML_SUBJECT-Zuordnung in PingOne. E-Mail (Arbeit) ist ein sinnvoller Wert für Testkonfigurationen mit PingOne integriertes Verzeichnis.

- Benutzer in PingOne Mit einer E-Mail-Adresse, die ein Pluszeichen enthält, kann es sein, dass sie sich nicht bei IAM Identity Center anmelden können. Es werden Fehler wie `'SAML_215'` oder `'Invalid input'` angezeigt. Um dieses Problem zu beheben, können Sie in PingOne, wählen Sie unter Attributzuordnungen die Option Erweitert für die SAML_SUBJECT-Zuordnung aus. Stellen Sie dann das Name-ID-Format für das Senden an SP ein: auf urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddressim Drop-down-Menü.

Schritt 1: Aktivieren Sie die Bereitstellung im IAM Identity Center

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

Um die automatische Bereitstellung in 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 den SCIM-Endpunkt und das Zugriffstoken. Sie müssen diese später einfügen, wenn Sie die Bereitstellung in Ihrem IdP konfigurieren.

   a. SCIM-Endpunkt — Zum Beispiel https://scim. *us-east-2*.amazonaws.com/ /scim/v2 *11111111111-2222-3333-4444-555555555555*

   b. Zugriffstoken — Wählen Sie Token anzeigen, um den Wert zu kopieren.

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

werden diese Werte eingeben, um die automatische Bereitstellung in Ihrem IdP später in diesem Tutorial zu konfigurieren.

5. Klicken Sie auf Close (Schließen).

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

Schritt 2: Konfigurieren Sie die Bereitstellung in PingOne

Verwenden Sie das folgende Verfahren in der PingOne IAM Identity Center-Anwendung, um die Bereitstellung mit IAM Identity Center zu ermöglichen. Bei diesem Verfahren wird davon ausgegangen, dass Sie das bereits hinzugefügt haben PingOne IAM Identity Center-Anwendung zu Ihrer PingOne Admin-Portal. Falls Sie dies noch nicht getan haben, finden Sie weitere Informationen zur Voraussetzungen Konfiguration der SCIM-Bereitstellung unter und führen Sie es anschließend aus.

So konfigurieren Sie die Bereitstellung in PingOne

1. Öffnen Sie 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 zum Ende der Seite. Wählen Sie unter Benutzerbereitstellung den vollständigen Link aus, um zur Benutzerbereitstellungskonfiguration Ihrer Verbindung zu gelangen.
3. Wählen Sie auf der Seite mit den Anweisungen zur Bereitstellung die Option Weiter zum nächsten Schritt aus.
4. Im vorherigen Verfahren haben Sie den SCIM-Endpunktwert in IAM Identity Center kopiert. Fügen Sie diesen Wert in das SCIM-URL-Feld im PingOne IAM Identity Center-Anwendung. Außerdem haben Sie im vorherigen Verfahren den Wert des Zugriffstokens in IAM Identity Center kopiert. Fügen Sie diesen Wert in das Feld ACCESS_TOKEN im PingOne IAM Identity Center-Anwendung.
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. Folgen Sie dabei den Anweisungen weiter oben auf dieser Seite. Überlegungen Wählen Sie dann Weiter zum nächsten Schritt.

7. Auf dem PingOne Nehmen Sie auf der Seite App-Anpassung — IAM Identity Center die 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 das Single Sign-On bei IAM Identity Center aktivieren möchten. Wählen Sie Weiter zum nächsten Schritt.
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 wird auf der Benutzerseite angezeigt. Diese Benutzer können jetzt Konten und Anwendungen in IAM Identity Center zugewiesen werden.

    Denken Sie daran PingOne unterstützt nicht die Bereitstellung von Gruppen oder Gruppenmitgliedschaften über SCIM. Kontakt Ping für weitere Informationen.

(Optional) Schritt 3: Konfigurieren Sie Benutzerattribute in PingOne für die Zugriffskontrolle im IAM Identity Center

Dies ist ein optionales Verfahren für PingOne wenn Sie Attribute für IAM Identity Center konfigurieren möchten, um den Zugriff auf Ihre AWS Ressourcen zu verwalten. Die Attribute, die Sie definieren in PingOne wird in einer SAML-Assertion an IAM Identity Center übergeben. Anschließend erstellen Sie in IAM Identity Center einen Berechtigungssatz, um den Zugriff auf der Grundlage der Attribute zu verwalten, von denen Sie übergeben haben PingOne.

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.

Um Benutzerattribute zu konfigurieren PingOne für die Zugriffskontrolle im IAM Identity Center

1. Öffnen Sie 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 möchten.

   a. Geben `https://aws.amazon.com/SAML/Attributes/AccessControl:`*`AttributeName`* Sie im Feld Anwendungsattribut den Wert ein. *`AttributeName`*Ersetzen Sie es 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 PingOne Verzeichnis. Zum Beispiel E-Mail (Arbeit).

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

(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.

Fehlerbehebung

Für allgemeine SCIM- und SAML-Problembehebungen mit PingOne, finden Sie in den folgenden Abschnitten:

- Bestimmte Benutzer können sich von einem externen SCIM-Anbieter nicht mit dem IAM Identity Center synchronisieren
- Probleme mit dem Inhalt von SAML-Assertionen, die von IAM Identity Center erstellt wurden
- Beim Bereitstellen von Benutzern oder Gruppen mit einem externen Identitätsanbieter ist ein Fehler beim Duplizieren von Benutzern oder Gruppen aufgetreten
- Weitere Informationen zu PingOne, siehe PingOne Dokumentation.

Die folgenden Ressourcen können Ihnen bei der Problembehebung bei der Arbeit mit helfen AWS:

- AWS re:Post- Hier finden Sie weitere Ressourcen FAQs und Links zu diesen, die Ihnen bei der Behebung von Problemen helfen.
- AWS Support- Holen Sie sich technischen Support

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 Ihre Organisation einen anderen Identitätsanbieter wieMicrosoft 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 eine IAM Identity Center-Organisationsinstanz, um einen Administratorbenutzer einzurichten und zu testen. Dieser Administratorbenutzer erstellt und verwaltet Benutzer und Gruppen und gewährt AWS Zugriff mit Berechtigungssätzen. In den nächsten Schritten erstellen Sie Folgendes:

- Ein Administratorbenutzer mit dem Namen *`Nikki Wolf`*
- Eine Gruppe mit dem Namen *`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 Benutzern Zugriff auf die Anwendung gewähren möchten, können Sie alternativ Schritt 1 dieses Verfahrens ausführen und den Anwendungszugriff konfigurieren.

Voraussetzungen

Die folgenden Voraussetzungen sind erforderlich, um dieses Tutorial abzuschließen:

- IAM Identity Center aktivierenund über eine Organisationsinstanz von IAM Identity Center verfügen.
  - Wenn Sie über eine Kontoinstanz von IAM Identity Center verfügen, können Sie Benutzer und Gruppen erstellen und ihnen Zugriff auf Anwendungen gewähren. Weitere Informationen finden Sie unter Anwendungszugriff.
- Melden Sie sich bei der IAM Identity Center-Konsole an AWS-Managementkonsole und greifen Sie entweder wie folgt auf die IAM Identity Center-Konsole zu:
  - 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.
    - Weitere Hilfe bei der Anmeldung finden AWS-Anmeldung Sie in der AWS-Managementkonsole Anleitung.
- Sie können die Multi-Faktor-Authentifizierung für Ihre IAM Identity Center-Benutzer konfigurieren. Weitere Informationen finden Sie unter MFA im IAM Identity Center konfigurieren.

Schritt 1: Fügen Sie einen Benutzer hinzu

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

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 Einladung, dem IAM Identity Center beizutreten. Die E-Mail stammt entweder von `no-reply@signin.aws` oder`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.

4. 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 zu erteilen*`Nikki`*.

   Wählen Sie 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

5. Wählen Sie im Bereich Gruppen die Schaltfläche Aktualisieren aus. Die *Admin team* Gruppe wird in der Liste angezeigt.

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

6. 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 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 fügen Sie Administratorberechtigungen für die *Admin team* Gruppe hinzu, sodass diese *Nikki* auf Ressourcen zugreifen kann.

Schritt 2: Fügen Sie Administratorberechtigungen hinzu

> **Important**
>
> Folgen Sie diesen Schritten nur, wenn Sie eine Organisationsinstanz von IAM Identity Center aktiviert haben.

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 team* Gruppe 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 zum Erstellen 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 aus. 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 *`Admin team`* Gruppe und der *`AdministratorAccess`* Berechtigungssatz ausgewählt sind, und klicken Sie dann auf Absenden.

Die Seite wird mit einer Meldung aktualisiert, dass Ihre 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 testen Sie den *Nikki's* Zugriff, indem Sie sich mit ihren Administratoranmeldedaten beim AWS Zugriffsportal anmelden und ihr Passwort festlegen. Melden Sie sich jetzt von der Konsole ab.

Schritt 3: Testen des Benutzerzugriffs

Da *Nikki Wolf* es sich nun um einen Benutzer in Ihrer Organisation handelt, kann er sich anmelden und auf die Ressourcen zugreifen, für die ihm gemäß seinem Berechtigungssatz Berechtigungen erteilt wurden. Um zu überprüfen, ob der Benutzer korrekt konfiguriert ist, verwenden Sie im nächsten Schritt *Nikki's* Anmeldeinformationen, um sich anzumelden und sein Passwort einzurichten. Als Sie den Benutzer *Nikki Wolf* in Schritt 1 hinzugefügt haben, haben Sie ausgewählt, dass Sie eine E-Mail mit Anweisungen zur Einrichtung des Passworts *Nikki* erhalten möchten. 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 den *Nikki's* Benutzernamen und die URL des AWS Zugriffsportals, mit denen sie sich bei der Organisation anmelden. Notieren Sie sich diese Informationen für future Verwendung.

Sie werden zur Anmeldeseite für neue Benutzer weitergeleitet, auf der Sie *Nikki's* ein Passwort festlegen und ihr MFA-Gerät registrieren können.

2. Nachdem Sie *Nikki's* das Passwort festgelegt haben, werden Sie zur Anmeldeseite weitergeleitet. Geben Sie ein *nikkiw* und wählen Sie Weiter. Geben Sie dann *Nikki's* das Passwort ein und wählen Sie Anmelden.
3. Das AWS Zugriffsportal 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 oder AWS CLIAWS SDKs.
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 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.

Video-Tutorials

Als zusätzliche Ressource können Sie diese Video-Tutorials verwenden, um mehr über die Einrichtung externer Identitätsanbieter zu erfahren:

- Migration zwischen externen Identitätsanbietern in AWS IAM Identity Center
- Föderieren Sie Ihre bestehende AWS IAM Identity Center Instanz mit Microsoft Entra ID

Richten Sie Ihre Belegschaft im IAM Identity Center ein

IAM Identity Center ist die AWS Lösung, um die Benutzer Ihrer Belegschaft mit AWS verwalteten Anwendungen wie Amazon Q Developer und Amazon Quick Suite sowie anderen AWS Ressourcen zu verbinden. Sie können Ihren bestehenden Identitätsanbieter verbinden und Benutzer und Gruppen aus Ihrem Verzeichnis synchronisieren oder Ihre Benutzer direkt im IAM Identity Center erstellen und verwalten.

Verwenden Sie IAM bereits für den Zugriff auf? AWS-Konten

Sie müssen keine Änderungen an Ihren aktuellen AWS-Konto Workflows vornehmen, um IAM Identity Center für den Zugriff auf AWS verwaltete Anwendungen zu verwenden. Wenn Sie den Verbund mit IAM für den AWS-Konto Zugriff verwenden, können Ihre Benutzer weiterhin auf die gleiche AWS-Konten Weise zugreifen, wie sie es immer getan haben, und Sie können weiterhin Ihre vorhandenen Workflows verwenden, um diesen Zugriff zu verwalten.

Wählen Sie den Ansatz, der am besten zur Identitätsmanagementstrategie und zur vorhandenen Infrastruktur Ihres Unternehmens passt.

Themen

- Benutzer, Gruppen und Bereitstellung im IAM Identity Center
- Verwaltung Ihrer Identitätsquelle
- Benutzer im Identity Center-Verzeichnis verwalten

Benutzer, Gruppen und Bereitstellung im IAM Identity Center

Mit IAM Identity Center können Sie steuern, wer sich anmelden kann und auf welche Ressourcen sie zugreifen können. Ein Benutzer muss über die erforderlichen Berechtigungen verfügen, um sich anmelden zu können. Sie können dann nur Benutzern oder Gruppen Zugriff zuweisen, die über die entsprechenden Berechtigungen verfügen. Erfahren Sie mehr über Benutzer, Gruppen und Bereitstellung in IAM Identity Center.

Eindeutigkeit von Benutzername und E-Mail-Adresse

Für IAM Identity Center muss jeder Benutzer einen eindeutigen Benutzernamen haben. Der Benutzername ist die primäre Kennung des Benutzers. Der Benutzername muss nicht mit der E-Mail-

Adresse des Benutzers übereinstimmen. IAM Identity Center setzt voraus, 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 keine verschachtelten Gruppen (eine Gruppe innerhalb einer Gruppe). 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.

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 Ihre Identitätsquelle mit IAM Identity Center verbinden. Mit IAM Identity Center können Sie Benutzern und Gruppen Zugriff auf verbundene Anwendungen zuweisen und. AWS-Konten

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

Deprovisionierung für Benutzer und Gruppen

Bei der Deprovisionierung werden Benutzer- und Gruppeninformationen aus dem IAM Identity Center entfernt.

Wenn Sie Active Directory oder einen externen Identitätsanbieter mit IAM Identity Center verwenden, sollten Sie Benutzer und Gruppen aus diesen Identitätsquellen und nicht aus IAM Identity Center entfernen. Durch das Löschen von IAM Identity Center-Benutzern und -Gruppen werden sie nicht vollständig entfernt, wenn Ihre Identitätsquelle Active Directory oder ein externer Identitätsanbieter ist.

Wenn Sie die Bereitstellung von IAM Identity Center-Benutzern oder -Gruppen aufheben müssen, sollten Sie zunächst alle Zuweisungen von Berechtigungssätzen oder Anwendungen zu den Benutzern oder Gruppen entfernen, für die Sie die Bereitstellung aufheben möchten. Andernfalls verfügen Sie in Ihrem IAM Identity Center über nicht zugewiesene Berechtigungssätze und Anwendungszuweisungen.

Verwaltung Ihrer 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 Anwendungen oder AWS-Konten beides zu gewähren.

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

- Externer Identitätsanbieter — Wählen Sie diese Option, wenn Sie Benutzer in einem externen Identitätsanbieter (IdP) wie Okta oder Microsoft Entra ID verwalten möchten.
- Ihr AWS lokales oder verwaltetes Active Directory — Wählen Sie diese Option, wenn Sie Ihre Active Directory (AD) Verbindung herstellen möchten.
- Identity Center-Verzeichnis — Wenn Sie IAM Identity Center zum ersten Mal aktivieren, wird es automatisch mit einem Identity Center-Verzeichnis als Standard-Identitätsquelle konfiguriert, sofern Sie keine andere Identitätsquelle wählen. Mit dem Identity Center-Verzeichnis erstellen Sie Ihre Benutzer und Gruppen und weisen deren Zugriffsebene Ihren AWS-Konten Anwendungen zu.

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

Themen

Überlegungen zur Änderung Ihrer Identitätsquelle

Sie können Ihre Identitätsquelle zwar jederzeit ändern, wir empfehlen Ihnen jedoch, darüber nachzudenken, wie sich diese Änderung auf Ihre aktuelle Bereitstellung auswirken könnte.

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

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

Wechseln zwischen dem IAM Identity Center-Verzeichnis und Active Directory

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

Important

Wenn Sie Ihren Identitätsquellentyp in IAM Identity Center zu oder von Active Directory ändern, beachten Sie, dass sich die Identity Store-ID ändert. Dies kann folgende Auswirkungen haben:

- Ihre Standard-URL für das AWS Zugriffsportal wird sich ändern. Sie müssen die neue URL Ihren Mitarbeitern mitteilen und die Lesezeichen, Gatewall- oder Firewall-Zulassungslisten sowie Konfigurationen, in denen auf diese URL verwiesen wird, aktualisieren. Wir empfehlen Ihnen, diese Änderung in einem geplanten Wartungsfenster vorzunehmen, um Störungen für Ihre Benutzer so gering wie möglich zu halten.
- Wenn Sie einen vom Kunden verwalteten KMS-Schlüssel für die Verschlüsselung im Ruhezustand in IAM Identity Center verwenden und die KMS-Schlüsselrichtlinie mit dem Verschlüsselungskontext konfiguriert haben, beachten Sie, dass sich der Verschlüsselungskontext für den Identity Store ändern wird. Im Identity Store-ARN „arn:aws:identitystore: :123456789012:identitystore/d-922763e9b3" ist „d-922763e9b3" beispielsweise die Identity Store-ID. Um Serviceunterbrechungen während dieser Umstellung zu vermeiden, ändern Sie Ihre KMS-Schlüsselrichtlinie vorübergehend so, dass sie ein Platzhaltermuster verwendet: „arn:aws:identitystore: :123456789012:identitystore/*“.

Wenn Sie bereits Benutzer und Gruppen im Identity Center-Standardverzeichnis verwalten, sollten Sie Folgendes beachten:

- Zuweisungen entfernt und Benutzer und Gruppen gelöscht — Wenn Sie Ihre Identitätsquelle auf 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 aus Active Directory mit dem 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 die entsprechenden Zuweisungen auch in IAM Identity Center gelöscht. Wenn in Active Directory Identitäten gelöscht werden (entweder in Active Directory oder in den synchronisierten Identitäten), werden die entsprechenden Zuweisungen jedoch nicht gelöscht.
- Keine ausgehende Synchronisierung für APIs — Wenn Sie Active Directory als Identitätsquelle verwenden, empfehlen wir, die Optionen Erstellen, Aktualisieren und Löschen mit Vorsicht zu verwenden. APIs IAM Identity Center unterstützt keine ausgehende Synchronisation, sodass Ihre Identitätsquelle nicht automatisch mit den Änderungen aktualisiert wird, die Sie an Benutzern oder Gruppen vornehmen, die diese verwenden. APIs
- Die URL des Zugriffsportals wird sich ändern — Wenn Sie Ihre Identitätsquelle zwischen IAM Identity Center und Active Directory ändern, ändert sich auch die URL für das AWS Zugriffsportal.
- Wenn Benutzer in der IAM Identity Center-Konsole mithilfe von Identity Store gelöscht oder deaktiviert werden APIs, können Benutzer mit aktiven Sitzungen weiterhin auf integrierte Anwendungen und Konten zugreifen. Informationen zur Dauer der Authentifizierungssitzung und zum Benutzerverhalten finden Sie unterGrundlegendes zu Authentifizierungssitzungen in IAM Identity Center.

Informationen darüber, wie IAM Identity Center Benutzer und Gruppen bereitstellt, finden Sie unterMicrosoft ADVerzeichnis.

Wechsel 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 beachten:

- Zuweisungen und Mitgliedschaften funktionieren mit korrekten Assertions — Ihre Benutzerzuweisungen, Gruppenzuweisungen und Gruppenmitgliedschaften funktionieren weiterhin, solange der neue IdP die richtigen Assertions sendet (z. B. den SAML-Namen). IDs Diese Assertions müssen mit den Benutzernamen und Gruppen in 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 Identity Provider erst in IAM Identity Center übernommen, 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 auf die Verwendung von IAM Identity Center zurücksetzen. Siehe Wechsel von einem externen IdP zu IAM Identity Center.
- Bestehende Benutzersitzungen werden nach Ablauf der Sitzungsdauer gesperrt. Sobald Sie Ihre Identitätsquelle auf einen externen Identitätsanbieter umgestellt haben, bleiben aktive Benutzersitzungen für den Rest der in der Konsole konfigurierten maximalen Sitzungsdauer bestehen. Wenn die Sitzungsdauer des AWS Access Portals beispielsweise auf acht Stunden festgelegt ist und Sie die Identitätsquelle in der vierten Stunde geändert haben, bleiben aktive Benutzersitzungen für weitere vier Stunden bestehen. Informationen zum Widerrufen von Benutzersitzungen finden Sie unterthe section called “Beenden Sie aktive Sitzungen für Workforce-Benutzer”.

  Wenn Benutzer in der IAM Identity Center-Konsole mithilfe von Identity Store gelöscht oder deaktiviert werden APIs, können Benutzer mit aktiven Sitzungen weiterhin auf integrierte Anwendungen und Konten zugreifen. Informationen zur Dauer der Authentifizierungssitzung und zum Benutzerverhalten finden Sie unterGrundlegendes zu Authentifizierungssitzungen in IAM Identity Center.

  > **Note**
  >
  > Sie können Benutzersitzungen nicht von der IAM Identity Center-Konsole aus widerrufen, nachdem Sie den Benutzer gelöscht haben.

Informationen darüber, wie IAM Identity Center Benutzer und Gruppen bereitstellt, finden Sie unter. Externe Identitätsanbieter

Wechsel von einem externen IdP zu IAM Identity Center

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

- IAM Identity Center behält alle Ihre Zuweisungen bei.
- Kennwortzurücksetzung erzwingen — Benutzer, die Passwörter in IAM Identity Center hatten, können sich weiterhin mit ihren alten Passwörtern anmelden. Für Benutzer, die sich im externen IdP und nicht im IAM Identity Center befanden, muss ein Administrator ein Zurücksetzen des Passworts erzwingen.
- Bestehende Benutzersitzungen werden nach Ablauf der Sitzungsdauer gesperrt. Sobald Sie Ihre Identitätsquelle auf IAM Identity Center ändern, bleiben aktive Benutzersitzungen für die verbleibende Dauer der in der Konsole konfigurierten maximalen Sitzungsdauer bestehen. Wenn die Dauer der AWS Access-Portal-Sitzung beispielsweise acht Stunden beträgt und Sie die Identitätsquelle in der vierten Stunde geändert haben, laufen aktive Benutzersitzungen weitere vier Stunden weiter. Informationen zum Widerrufen von Benutzersitzungen finden Sie unterthe section called “Beenden Sie aktive Sitzungen für Workforce-Benutzer”.

  Wenn Benutzer in der IAM Identity Center-Konsole mithilfe von Identity Store gelöscht oder deaktiviert werden APIs, können Benutzer mit aktiven Sitzungen weiterhin auf integrierte Anwendungen und Konten zugreifen. Informationen zur Dauer der Authentifizierungssitzung und zum Benutzerverhalten finden Sie unterGrundlegendes zu Authentifizierungssitzungen in IAM Identity Center.

  > **Note**
  >
  > Sie können Benutzersitzungen nicht mehr von der IAM Identity Center-Konsole aus widerrufen, nachdem Sie den Benutzer gelöscht haben.

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

Von einem externen IdP zu einem anderen externen IdP wechseln

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

- Aufgaben und Mitgliedschaften funktionieren mit den richtigen Assertions — IAM Identity Center behält all Ihre Zuweisungen bei. Die Benutzerzuweisungen, Gruppenzuweisungen und Gruppenmitgliedschaften funktionieren weiterhin, solange der neue IdP die richtigen Assertions sendet (z. B. den SAML-Namen). IDs

  Diese Assertionen müssen mit den Benutzernamen in IAM Identity Center übereinstimmen, wenn sich Ihre Benutzer über den neuen externen IdP authentifizieren.
- SCIM-Bereitstellung — Wenn Sie SCIM für die Bereitstellung im IAM Identity Center verwenden, empfehlen wir Ihnen, die IdP-spezifischen Informationen in diesem Handbuch und die vom IdP bereitgestellte Dokumentation zu lesen, um sicherzustellen, dass der neue Anbieter Benutzer und Gruppen korrekt zuordnet, wenn SCIM aktiviert ist.
- Bestehende Benutzersitzungen werden nach Ablauf der Sitzungsdauer gesperrt — Sobald Sie Ihre Identitätsquelle auf einen anderen externen Identitätsanbieter ändern, bleiben aktive Benutzersitzungen für die verbleibende Dauer der in der Konsole konfigurierten maximalen Sitzungsdauer bestehen. Wenn die Dauer der AWS Access-Portal-Sitzung beispielsweise acht Stunden beträgt und Sie die Identitätsquelle in der vierten Stunde geändert haben, bleiben aktive Benutzersitzungen für weitere vier Stunden bestehen. Informationen zum Widerrufen von Benutzersitzungen finden Sie unterthe section called “Beenden Sie aktive Sitzungen für Workforce-Benutzer”.

  Wenn Benutzer in der IAM Identity Center-Konsole mithilfe von Identity Store gelöscht oder deaktiviert werden APIs, können Benutzer mit aktiven Sitzungen weiterhin auf integrierte Anwendungen und Konten zugreifen. Informationen zur Dauer der Authentifizierungssitzung und zum Benutzerverhalten finden Sie unterGrundlegendes zu Authentifizierungssitzungen in IAM Identity Center.

  > **Note**
  >
  > Sie können Benutzersitzungen nicht von der IAM Identity Center-Konsole aus widerrufen, nachdem Sie den Benutzer gelöscht haben.

Informationen darüber, wie IAM Identity Center Benutzer und Gruppen bereitstellt, finden Sie unter. Externe Identitätsanbieter

Zwischen Active Directory und einem externen IdP wechseln

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

- Benutzer, Gruppen und Zuweisungen werden gelöscht — Alle Benutzer, Gruppen und Zuweisungen werden aus IAM Identity Center gelöscht. Weder im externen IdP noch in Active Directory sind Benutzer- oder Gruppeninformationen betroffen.
- Benutzer bereitstellen — 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.
- Wenn Benutzer in der IAM Identity Center-Konsole mithilfe von Identity Store gelöscht oder deaktiviert werden APIs, können Benutzer mit aktiven Sitzungen weiterhin auf integrierte Anwendungen und Konten zugreifen. Informationen zur Dauer der Authentifizierungssitzung und zum Benutzerverhalten finden Sie unterGrundlegendes zu Authentifizierungssitzungen in IAM Identity Center.

Informationen darüber, wie IAM Identity Center Benutzer und Gruppen bereitstellt, finden Sie unterMicrosoft ADVerzeichnis.

Ändern Sie Ihre Identitätsquelle

Das folgende Verfahren beschreibt, wie Sie von einem Verzeichnis, das IAM Identity Center bereitstellt (das Identity Center-Standardverzeichnis), zu Active Directory oder einem externen Identitätsanbieter wechseln oder umgekehrt. Bevor Sie fortfahren, überprüfen Sie die Informationen unterÜberlegungen zur Änderung Ihrer Identitätsquelle. Um dieses Verfahren abzuschließen, benötigen Sie eine Organisationsinstanz von IAM Identity Center. Weitere Informationen finden Sie unter Organisations- und Kontoinstanzen von IAM Identity Center.

> **Warning**
>
> Je nach Ihrer aktuellen Bereitstellung werden durch diese Änderung alle Benutzer- und Gruppenzuweisungen entfernt, die Sie in IAM Identity Center konfiguriert haben. Durch diese Änderung werden auch die IAM-Rollen mit dem Berechtigungssatz aus Ihren entfernt. AWS-Konten Daher müssen Sie möglicherweise Ihre Ressourcenrichtlinien aktualisieren und sollten sicherstellen, dass dadurch Ihr Zugriff auf AWS KMS Schlüssel und Amazon EKS-Cluster nicht beeinträchtigt wird. Weitere Informationen hierzu finden Sie unter Referenzieren von Berechtigungssätzen in Ressourcenrichtlinien, Amazon EKS-Cluster-Konfigurationszuordnungen und AWS KMS wichtigen Richtlinien.
> In diesem Fall verlieren alle Benutzer und Gruppen, einschließlich des Administratorbenutzers in IAM Identity Center, den Single Sign-On-Zugriff auf ihre AWS-Konten Anwendungen.

Um Ihre Identitätsquelle zu ändern

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite Einstellungen den Tab Identitätsquelle aus. Wählen Sie Aktionen und dann Identitätsquelle ändern aus.
4. Wählen Sie unter Identitätsquelle auswählen die Quelle aus, zu der Sie wechseln möchten, und klicken Sie dann auf Weiter.

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

   > **Important**
   >
   > Wenn Sie Ihre Identitätsquelle zu oder von 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, empfehlen wir Ihnen, die Schritte unter zu befolgen. Wie stelle ich eine Verbindung zu einem externen Identitätsanbieter her

5. Nachdem Sie den Haftungsausschluss gelesen haben und bereit sind, fortzufahren, geben Sie ACCEPT ein.
6. Wählen Sie „Identitätsquelle ändern“. Wenn Sie Ihre Identitätsquelle auf Active Directory ändern, fahren Sie mit dem nächsten Schritt fort.
7. Wenn Sie Ihre Identitätsquelle auf Active Directory ändern, gelangen Sie zur Seite Einstellungen. Führen Sie auf der Seite „Einstellungen“ einen der folgenden Schritte aus:

   - Wählen Sie „Geführte Installation starten“. Informationen darüber, wie Sie den geführten Einrichtungsprozess abschließen, finden Sie unterGeführte Einrichtung.
   - Wählen Sie im Abschnitt Identitätsquelle die Option Aktionen und anschließend Synchronisierung verwalten aus, um Ihren Synchronisierungsbereich und die Liste der zu synchronisierenden Benutzer und Gruppen zu konfigurieren.

Unterstützte Benutzer- und Gruppenattribute in IAM Identity Center

Dieses Handbuch enthält eine Referenz zur Unterstützung von SCIM-Attributen im IAM Identity Center. Es listet auf, welche Benutzer- und Gruppenattribute aus der SCIM-Spezifikation im IAM Identity Center-Identitätsspeicher unterstützt werden, und identifiziert bestimmte Attribute und Unterattribute, die nicht unterstützt werden.

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 sowohl durch manuelle Eingabe als auch durch automatische SCIM-Bereitstellung.

- Informationen zur SCIM-Spezifikation (System for Cross-Domain Identity Management) finden Sie unter /rfc7642. https://tools.ietf.org/html
- Informationen zur manuellen und automatischen Bereitstellung finden Sie unter. Bereitstellung, wenn Benutzer von einem externen IdP kommen
- Informationen zur Attributzuweisung finden Sie unterAttributzuordnungen zwischen dem IAM Identity Center und dem Verzeichnis externer Identitätsanbieter.

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 werden nicht unterstützt

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'`

Gruppenobjekte werden nicht unterstützt

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).

Externe Identitätsanbieter

Mit IAM Identity Center können Sie Ihre vorhandenen Personalidentitäten von externen Identitätsanbietern (IdPs) über die Protokolle Security Assertion Markup Language (SAML) 2.0 und System for Cross-Domain Identity Management (SCIM) verbinden. Auf diese Weise können sich Ihre Benutzer mit ihren Unternehmensanmeldedaten beim Access Portal anmelden. AWS 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.

Wenn Sie ein selbstverwaltetes Verzeichnis in Active Directory oder einem anderen verwenden AWS Managed Microsoft AD, finden Sie weitere Informationen unter. Microsoft ADVerzeichnis

> **Note**
>
> 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 Stellen Sie Benutzer und Gruppen von einem externen Identitätsanbieter mithilfe von SCIM bereit für Ihre Benutzer und Gruppen konfigurieren oder verwenden. Manuelles Provisioning Unabhängig davon, wie Sie Benutzer bereitstellen, leitet IAM Identity Center die AWS-Managementkonsole 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

Themen

- Wie stelle ich eine Verbindung zu einem externen Identitätsanbieter her
- Wie ändere ich die Metadaten eines externen Identitätsanbieters in IAM Identity Center
- Verwenden des SAML- und SCIM-Identitätsverbunds mit externen Identitätsanbietern
- SCIM-Profil und SAML 2.0-Implementierung

Wie stelle ich eine Verbindung zu einem externen Identitätsanbieter her

Für die unterstützten externen IdPs Geräte gelten unterschiedliche Voraussetzungen, Überlegungen und Bereitstellungsverfahren. Für mehrere IdPs sind step-by-step Tutorials verfügbar:

- CyberArk
- Google Workspace
- JumpCloud
- Microsoft Entra ID
- Okta
- OneLogin
- Ping-Identität

Weitere Informationen zu den Überlegungen für externe Geräte IdPs , die IAM Identity Center unterstützt, finden Sie unterVerwenden des SAML- und SCIM-Identitätsverbunds mit externen Identitätsanbietern.

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 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.

Wie ändere ich die Metadaten eines externen Identitätsanbieters in IAM Identity Center

Sie können die Metadaten Ihres externen Identitätsanbieters ändern, die Sie zuvor an das IAM Identity Center übermittelt haben. Diese Änderungen wirken sich auf die Fähigkeit Ihrer Benutzer aus, sich über IAM Identity Center anzumelden und auf AWS Ressourcen zuzugreifen. Im folgenden Verfahren wird beschrieben, wie Sie die Metadaten Ihres externen IdP aktualisieren, die im IAM Identity Center gespeichert sind. Um dieses Verfahren abzuschließen, benötigen Sie eine Organisationsinstanz von IAM Identity Center. Weitere Informationen finden Sie unter Organisations- und Kontoinstanzen von IAM Identity Center.

Um die Metadaten eines externen Identitätsanbieters zu ändern

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Identitätsquelle aus. Wählen Sie Aktionen und dann Authentifizierung verwalten aus.
4. Wählen Sie im Abschnitt Metadaten des Identitätsanbieters die Option IdP-Metadaten bearbeiten aus. Auf dieser Seite können Sie die Änderungen an der IdP-Anmelde-URL und/oder der IdP-Aussteller-URL für Ihren externen IdP vornehmen. Wählen Sie Änderungen speichern, wenn Sie alle erforderlichen Änderungen vorgenommen haben.

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) adressspezifikationskonforme („“) Zeichenfolge (/rfc2822 #section -3.4.1) sein. `name@domain.com` https://tools.ietf.org/html
  - 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.
  - IAM Identity Center unterstützt nicht das Signieren von SAML-Authentifizierungsanforderungen, die es an externe Empfänger sendet. IdPs

- SCIM
  - Die SCIM-Implementierung von IAM Identity Center basiert auf SCIM RFCs 7642 (https://tools.ietf.org/html/rfc7642), 7643 (/rfc7643) und 7644 (https://tools.ietf.org/html/rfc7644) sowie den Interoperabilitätsanforderungen, die im Entwurf des Basic SCIM Profile 1.0 vom März 2020 (#rfc https://tools.ietf.org/html.section.4) dargelegt wurden. FastFed https://openid.net/specs/fastfed-scim-1_0-02.html 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 Sie nach dem Ereignisnamen Login filtern ExternalId PDirectory
- IDP-spezifische Protokolle Debug-Protokolle and/or
- Behebung von Problemen mit IAM Identity Center

> **Note**
>
> Einige IdPs, wie die in derTutorials zu Identitätsquellen im IAM Identity Center, bieten eine vereinfachte Konfigurationserfahrung 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 and/or Endpunkte mit anderen Verbundansätzen 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-Managementkonsole 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. Stellen Sie Benutzer und Gruppen von einem externen Identitätsanbieter mithilfe von SCIM bereit Weitere Informationen zur SCIM-Implementierung von IAM Identity Center finden Sie im IAM Identity Center SCIM Implementation Developer Guide.

Themen

- Stellen Sie Benutzer und Gruppen von einem externen Identitätsanbieter mithilfe von SCIM bereit
- Wechseln Sie die SAML 2.0-Zertifikate

Stellen Sie Benutzer und Gruppen von einem externen Identitätsanbieter mithilfe von SCIM bereit

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

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 Tutorials zu Identitätsquellen im IAM Identity Center 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.
- Nachdem Sie die automatische Bereitstellung mit SCIM für Ihren IdP eingerichtet haben, können Sie in der IAM Identity Center-Konsole keine Benutzer mehr hinzufügen oder bearbeiten. Wenn Sie einen Benutzer hinzufügen oder ändern müssen, müssen Sie dies von Ihrem externen IdP oder Ihrer Identitätsquelle aus tun.

Weitere Informationen zur SCIM-Implementierung von IAM Identity Center finden Sie im IAM Identity Center SCIM Implementation Developer Guide.

Wie überwacht man den Ablauf des Zugriffstokens

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.

Generieren Sie ein 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 Aktivieren Sie 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.

Aktivieren Sie 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 Tutorials zu Identitätsquellen im IAM Identity Center 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 den SCIM-Endpunkt und das Zugriffstoken. Sie müssen diese später einfügen, wenn Sie die Bereitstellung in Ihrem IdP konfigurieren.

   a. SCIM-Endpunkt — Zum Beispiel https://scim. *us-east-2*.amazonaws.com/ /scim/v2 *11111111111-2222-3333-4444-555555555555*

   b. Zugriffstoken — Wählen Sie Token anzeigen, um den Wert zu kopieren.

> **Warning**
>
> Dies ist das einzige Mal, dass Sie den SCIM-Endpunkt und das Zugriffstoken abrufen können. Stellen Sie sicher, dass Sie diese Werte kopieren, bevor Sie fortfahren. Sie werden diese Werte eingeben, um die automatische Bereitstellung in Ihrem IdP später in diesem Tutorial zu konfigurieren.

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 Tutorials zu Identitätsquellen im IAM Identity Center Für Ihren IdP.

Löschen Sie 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.

Deaktivieren Sie 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 Löschen Sie 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.

Ein Zugriffstoken rotieren

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 unterGenerieren Sie ein 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 unterLöschen Sie 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.

Automatisch bereitgestellte Ressourcen prüfen und abgleichen

Mit SCIM können Sie automatisch Benutzer, Gruppen und Gruppenmitgliedschaften aus Ihrer Identitätsquelle für IAM Identity Center bereitstellen. Dieses Handbuch hilft Ihnen dabei, diese Ressourcen zu überprüfen und abzugleichen, um eine korrekte Synchronisation zu gewährleisten.

Warum sollten Sie Ihre Ressourcen prüfen?

Regelmäßige Prüfungen tragen dazu bei, dass Ihre Zugriffskontrollen korrekt bleiben und Ihr Identity Provider (IdP) ordnungsgemäß mit IAM Identity Center synchronisiert bleibt. Dies ist besonders wichtig für die Einhaltung von Sicherheitsbestimmungen und das Zugriffsmanagement.

Ressourcen, die Sie prüfen können:

- Benutzer
- Gruppen
- Gruppenmitgliedschaften

Sie können AWS Identity Store APIs- oder CLI-Befehle verwenden, um die Prüfung und den Abgleich durchzuführen. In den folgenden Beispielen AWS CLI werden Befehle verwendet. API-Alternativen finden Sie in den entsprechenden Vorgängen in der Identity Store-API-Referenz.

Wie prüft man Ressourcen

Im Folgenden finden Sie Beispiele dafür, wie Sie diese Ressourcen mithilfe von AWS CLI Befehlen prüfen können.

Stellen Sie vor Beginn sicher, dass Sie über Folgendes verfügen:

- Administratorzugriff auf IAM Identity Center.
- AWS CLI installiert und konfiguriert. Weitere Informationen finden Sie im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle.
- Erforderliche IAM-Berechtigungen für Identity Store-Befehle.

Schritt 1: Aktuelle Ressourcen auflisten

Sie können Ihre aktuellen Ressourcen mit dem anzeigen AWS CLI.

> **Note**
>
> Wenn Sie den verwenden AWS CLI, erfolgt die Seitennummerierung automatisch, sofern Sie nichts anderes angeben`--no-paginate`. Wenn Sie die API direkt aufrufen (z. B. mit einem SDK oder einem benutzerdefinierten Skript), behandeln Sie das `NextToken` in der Antwort. Dadurch wird sichergestellt, dass Sie alle Ergebnisse auf mehreren Seiten abrufen.

Example für Benutzer

```
aws identitystore list-users \
  --region REGION \
  --identity-store-id IDENTITY_STORE_ID
```

Example für Gruppen

```
aws identitystore list-groups \
  --region REGION \
  --identity-store-id IDENTITY_STORE_ID
```

Example für Gruppenmitgliedschaften

```
aws identitystore list-group-memberships \
  --region REGION \
  --identity-store-id IDENTITY_STORE_ID
  --group-id GROUP_ID
```

Schritt 2: Mit Ihrer Identitätsquelle vergleichen

Vergleichen Sie die aufgelisteten Ressourcen mit Ihrer Identitätsquelle, um etwaige Unstimmigkeiten zu ermitteln, z. B.:

- Fehlende Ressourcen, die in IAM Identity Center bereitgestellt werden sollten.
- Zusätzliche Ressourcen, die aus IAM Identity Center entfernt werden sollten.

Example für Benutzer

```
# Create missing users
aws identitystore create-user \
  --identity-store-id IDENTITY_STORE_ID \
  --user-name USERNAME \
  --display-name DISPLAY_NAME \
  --name GivenName=FIRST_NAME,FamilyName=LAST_NAME \
  --emails Value=EMAIL,Primary=true

# Delete extra users
aws identitystore delete-user \
  --identity-store-id IDENTITY_STORE_ID \
```

```
  --user-id USER_ID
```

Example für Gruppen

```
# Create missing groups
aws identitystore create-group \
  --identity-store-id IDENTITY_STORE_ID \
  [group attributes]

# Delete extra groups
aws identitystore delete-group \
  --identity-store-id IDENTITY_STORE_ID \
  --group-id GROUP_ID
```

Example für Gruppenmitgliedschaften

```
# Add missing members
aws identitystore create-group-membership \
  --identity-store-id IDENTITY_STORE_ID \
  --group-id GROUP_ID \
  --member-id '{"UserId": "USER_ID"}'

# Remove extra members
aws identitystore delete-group-membership \
  --identity-store-id IDENTITY_STORE_ID \
  --membership-id MEMBERSHIP_ID
```

Überlegungen

- Befehle unterliegen Dienstkontingenten und API-Drosselung.
- Wenn Sie beim Abgleich viele Unterschiede feststellen, nehmen Sie kleine, schrittweise Änderungen am AWS Identity Store vor. Auf diese Weise können Sie Fehler vermeiden, die mehrere Benutzer betreffen.
- Die SCIM-Synchronisierung kann Ihre manuellen Änderungen außer Kraft setzen. Überprüfe deine IdP-Einstellungen, um dieses Verhalten zu verstehen.

Manuelles Provisioning

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.

Wechseln Sie die SAML 2.0-Zertifikate

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, bei dem ein älteres Zertifikat durch ein neueres ersetzt wird, 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 in der Spalte Läuft ab neben jedem Zertifikat in der Liste farbige Statusanzeigesymbole 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 abgelaufen ist.
- Gelb — Zeigt an, dass ein Zertifikat in 90 Tagen oder weniger abläuft.
- Grün — Zeigt an, dass ein Zertifikat 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.

Microsoft ADVerzeichnis

Mit AWS IAM Identity Center können Sie ein selbstverwaltetes Verzeichnis in Active Directory (AD) oder ein Verzeichnis in mithilfe AWS Managed Microsoft AD von. 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 dem IAM Identity Center verbunden haben, können Sie Ihren AD-Benutzern oder -Gruppen Zugriff AWS-Konten auf Anwendungen oder beides gewähren.

AWS Directory Service hilft Ihnen bei der Einrichtung und Ausführung eines eigenständigen AWS Managed Microsoft AD Verzeichnisses, das in der AWS Cloud gehostet wird. Sie können es auch verwenden Directory Service , um Ihre AWS Ressourcen mit einem vorhandenen selbstverwalteten AD zu verbinden. Um die Konfiguration AWS Directory Service für die Verwendung mit Ihrem selbstverwalteten AD durchzuführen, müssen Sie zunächst Vertrauensbeziehungen einrichten, um die Authentifizierung auf die Cloud auszudehnen.

IAM Identity Center verwendet die von bereitgestellte Verbindung Directory Service , um die Passthrough-Authentifizierung für die AD-Quellinstanz durchzuführen. Wenn Sie IAM Identity Center AWS Managed Microsoft AD als Identitätsquelle verwenden, kann es mit Benutzern aus AWS Managed Microsoft AD oder von jeder Domain zusammenarbeiten, die über einen AD-Trust verbunden ist. Wenn Sie Ihre Benutzer in vier oder mehr Domänen suchen möchten, müssen Benutzer die `DOMAIN\user` Syntax als ihren Benutzernamen verwenden, wenn sie sich bei IAM Identity Center anmelden.

Hinweise

- Stellen Sie als Voraussetzung sicher, dass sich Ihr AD Connector oder Ihr Verzeichnis AWS Managed Microsoft AD in in in Ihrem AWS Organizations Verwaltungskonto Directory Service befindet.
- IAM Identity Center unterstützt SAMBA 4-basiertes Simple AD nicht als verbundenes Verzeichnis.

Eine Demonstration der Verwendung von Active Directory als Identitätsquelle für IAM Identity Center finden Sie im folgenden Video: YouTube

Verwenden von Active Directory als Identitätsquelle für AWS IAM Identity Center | Amazon Web Services

Überlegungen zur Verwendung von Active Directory

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

- Wenn Sie IAM Identity Center verwenden AWS Managed Microsoft AD, müssen Sie es dort aktivieren AWS-Region , wo Ihr AWS Managed Microsoft AD Verzeichnis eingerichtet ist. IAM Identity Center speichert die Zuweisungsdaten in derselben Region wie das Verzeichnis. Um IAM Identity Center zu verwalten, müssen Sie möglicherweise zu der Region wechseln, in der IAM Identity Center konfiguriert ist. Beachten Sie außerdem, dass das AWS Zugriffsportal dieselbe Zugriffs-URL wie Ihr Verzeichnis verwendet.
- Verwenden Sie ein Active Directory, das sich im Verwaltungskonto befindet:

  Sie müssen einen vorhandenen AD Connector oder ein AWS Managed Microsoft AD Verzeichnis eingerichtet haben AWS Directory Service, und es muss sich in Ihrem AWS Organizations Verwaltungskonto befinden. Sie können jeweils nur ein AD Connector Connector-Verzeichnis oder ein Verzeichnis verbinden. AWS Managed Microsoft AD Wenn Sie mehrere Domänen oder Gesamtstrukturen unterstützen müssen, verwenden Sie AWS Managed Microsoft AD. Weitere Informationen finden Sie unter:
  - Ein Verzeichnis mit dem IAM Identity Center Connect AWS Managed Microsoft AD
  - Ein selbstverwaltetes Verzeichnis in Active Directory mit IAM Identity Center Connect
- Verwenden Sie ein Active Directory, das sich im delegierten Administratorkonto befindet:

Wenn Sie planen, den 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 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.

Connect Active Directory und geben Sie einen Benutzer an

Wenn Sie Active Directory bereits 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.

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

AWS Managed Microsoft AD

1. Lesen Sie die Anleitung unterMicrosoft ADVerzeichnis.
2. Führen Sie die Schritte unter Ein Verzeichnis mit dem IAM Identity Center Connect AWS Managed Microsoft AD 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 Sie einen Administratorbenutzer mit IAM Identity Center.

Selbstverwaltetes Verzeichnis in Active Directory

1. Lesen Sie die Anleitung unterMicrosoft ADVerzeichnis.
2. Führen Sie die Schritte unter Ein selbstverwaltetes Verzeichnis in Active Directory mit IAM Identity Center Connect 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 Sie einen Administratorbenutzer mit IAM Identity Center.

Externer IdP

1. Lesen Sie die Anleitung unterExterne Identitätsanbieter.
2. Führen Sie die Schritte unter Wie stelle ich eine Verbindung zu einem externen Identitätsanbieter her aus.
3. Konfigurieren Sie Ihren IdP so, dass er Benutzer für das IAM Identity Center bereitstellt.

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

Synchronisieren Sie einen Administratorbenutzer mit IAM Identity Center

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

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“, klicken Sie auf „Aktionen“ und anschließend auf „Synchronisation verwalten“.
4. Wählen Sie auf der Seite „Synchronisation verwalten“ die Registerkarte „Benutzer“ und dann „Benutzer und Gruppen hinzufügen“ aus.
5. Geben Sie auf der Registerkarte Benutzer unter Benutzer den genauen Benutzernamen ein und wählen Sie Hinzufügen aus.
6. Gehen Sie unter Hinzugefügte Benutzer und Gruppen wie folgt vor:

a. Vergewissern Sie sich, dass der Benutzer, dem Sie Administratorrechte gewähren möchten, angegeben ist.

b. Aktivieren Sie das Kontrollkästchen links neben dem Benutzernamen.

c. Wählen Sie Absenden aus.

7. Auf der Seite „Synchronisation verwalten“ wird der von Ihnen angegebene Benutzer in der Liste „Synchronisierte Benutzer“ angezeigt.
8. Klicken Sie im Navigationsbereich auf Users (Benutzer).
9. Auf der Seite Benutzer kann es einige Zeit dauern, bis der von Ihnen angegebene Benutzer in der Liste erscheint. Wählen Sie das Aktualisierungssymbol, um die Benutzerliste zu aktualisieren.

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

Bereitstellung, wenn Benutzer aus Active Directory kommen

IAM Identity Center verwendet die von der bereitgestellte Verbindung, Directory Service um Benutzer-, Gruppen- und Mitgliedschaftsinformationen aus Ihrem Quellverzeichnis in Active Directory mit dem IAM Identity Center-Identitätsspeicher zu synchronisieren. Es werden keine Kennwortinformationen 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-Such-, Autorisierungs- und Zusammenarbeitsszenarien zu ermöglichen, ohne LDAP-Aktivitäten an das Quellverzeichnis in Active Directory zurückzugeben.

Weitere Informationen zur Bereitstellung finden Sie unter. Bereitstellung von Benutzern und Gruppen

Themen

- Ein Verzeichnis mit dem IAM Identity Center Connect AWS Managed Microsoft AD
- Ein selbstverwaltetes Verzeichnis in Active Directory mit IAM Identity Center Connect
- Attributzuordnungen zwischen dem IAM Identity Center und dem Verzeichnis externer Identitätsanbieter
- IAM Identity Center, konfigurierbare AD-Synchronisierung

Ein Verzeichnis mit dem IAM Identity Center Connect AWS Managed Microsoft AD

Gehen Sie wie folgt vor, um ein Verzeichnis, das von verwaltet wird AWS Managed Microsoft AD , mit dem IAM Identity Center AWS Directory Service zu verbinden.

So stellen Sie eine Verbindung AWS Managed Microsoft AD zum 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 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 Active Directory und dann Weiter aus.
5. Wählen Sie unter Active Directory verbinden ein Verzeichnis in AWS Managed Microsoft AD aus der Liste aus, und klicken Sie dann auf Weiter.
6. Überprüfen Sie unter Änderung bestätigen die Informationen, geben Sie ACCEPT ein, wenn Sie bereit sind, und wählen Sie dann Identitätsquelle ändern aus.

   > **Important**
   >
   > Um einen Benutzer in Active Directory als Administratorbenutzer in IAM Identity Center anzugeben, müssen Sie zuerst den Benutzer, dem Sie Administratorrechte aus Active Directory gewähren möchten, mit IAM Identity Center synchronisieren. Eine Schritt-für-Schritt-Anleitung hierzu finden Sie unter Synchronisieren Sie einen Administratorbenutzer mit IAM Identity Center.

Ein selbstverwaltetes Verzeichnis in Active Directory mit IAM Identity Center Connect

Benutzer in Ihrem selbstverwalteten Verzeichnis in Active Directory (AD) können auch über Single Sign-On auf Anwendungen im AWS-Konten Zugriffsportal zugreifen. AWS Um den Single Sign-On-Zugriff für diese Benutzer zu konfigurieren, können Sie einen der folgenden Schritte ausführen:

- Eine bidirektionale Vertrauensstellung einrichten — Wenn wechselseitige Vertrauensstellungen zwischen AWS Managed Microsoft AD und einem selbstverwalteten Verzeichnis in AD eingerichtet werden, können sich Benutzer in Ihrem selbstverwalteten Verzeichnis in AD mit ihren Unternehmensanmeldeinformationen bei verschiedenen AWS Diensten 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 und Benutzer- und Gruppenmetadaten synchronisiert werden können. IAM Identity Center verwendet diese Metadaten, wenn es Zugriff auf Berechtigungssätze oder Anwendungen zuweist. Benutzer- und Gruppenmetadaten werden auch von Anwendungen für die Zusammenarbeit verwendet, z. B. wenn Sie ein Dashboard mit einem anderen Benutzer oder einer anderen Gruppe teilen. Das Vertrauen von Directory Service Microsoft Active Directory zu Ihrer Domain ermöglicht es IAM Identity Center, Ihrer Domain bei der Authentifizierung zu vertrauen. Das Vertrauen in die entgegengesetzte Richtung gewährt AWS Berechtigungen zum Lesen von Benutzer- und Gruppenmetadaten.

  Weitere Informationen zum Einrichten einer bidirektionalen Vertrauensstellung finden Sie unter Wann sollte eine Vertrauensstellung eingerichtet werden? im AWS Directory Service Administratorhandbuch.

  > **Note**
  >
  > Um AWS Anwendungen wie IAM Identity Center zum Lesen von Directory Service Verzeichnisbenutzern aus vertrauenswürdigen Domänen verwenden zu können, benötigen die Directory Service Konten Berechtigungen für das userAccountControl Attribut der vertrauenswürdigen Benutzer. Ohne Leseberechtigungen für dieses Attribut können AWS Anwendungen nicht feststellen, ob das Konto aktiviert oder deaktiviert ist. Lesezugriff auf dieses Attribut wird standardmäßig gewährt, wenn eine Vertrauensstellung erstellt wird. Wenn Sie den Zugriff auf dieses Attribut verweigern (nicht empfohlen), verhindern Sie, dass Anwendungen wie Identity Center vertrauenswürdige Benutzer lesen können. Die Lösung besteht darin, den Lesezugriff auf das `userAccountControl` Attribut der AWS Dienstkonten unter der AWS reservierten Organisationseinheit (mit dem Präfix AWS_) ausdrücklich zuzulassen.

- Erstellen Sie einen AD-Connector — AD Connector ist ein Verzeichnis-Gateway, das Verzeichnisanfragen an Ihr selbstverwaltetes AD umleiten kann, ohne Informationen in der Cloud zwischenzuspeichern. Weitere Informationen finden Sie unter Connect einem Verzeichnis

herstellen im AWS Directory Service Administratorhandbuch. Bei der Verwendung von AD Connector sollten Sie Folgendes beachten:

- Wenn Sie IAM Identity Center mit einem AD Connector Connector-Verzeichnis verbinden, müssen alle future Benutzerpasswörter von AD aus zurückgesetzt werden. Das bedeutet, dass Benutzer ihre Passwörter nicht über das AWS Zugriffsportal zurücksetzen können.
- Wenn Sie AD Connector verwenden, um Ihren Active Directory-Domänendienst mit IAM Identity Center zu verbinden, hat IAM Identity Center nur Zugriff auf die Benutzer und Gruppen der einzelnen Domäne, an die AD Connector angehängt ist. Wenn Sie mehrere Domänen oder Gesamtstrukturen unterstützen müssen, verwenden Sie Directory Service Microsoft Active Directory.

> **Note**
>
> IAM Identity Center funktioniert nicht mit SAMBA4 basierten Simple AD AD-Verzeichnissen.

Attributzuordnungen zwischen dem IAM Identity Center und dem Verzeichnis externer Identitätsanbieter

Attributzuordnungen werden verwendet, um Attributtypen, die in IAM Identity Center vorhanden sind, ähnlichen Attributen in Ihrer externen Identitätsquelle zuzuordnen, z. B., und. Google Workspace Microsoft Active Directory (AD) Okta IAM Identity Center ruft Benutzerattribute aus Ihrer Identitätsquelle ab und ordnet sie den IAM Identity Center-Benutzerattributen zu.

Wenn Ihr IAM Identity Center so synchronisiert ist, dass es einen externen Identitätsanbieter (IdP) wie Google WorkspaceOkta, oder Ping als Identitätsquelle verwendet, müssen Sie Ihre Attribute in Ihrem IdP zuordnen.

IAM Identity Center füllt eine Reihe von Attributen für Sie auf der Registerkarte Attributzuordnungen auf der Konfigurationsseite automatisch aus. IAM Identity Center verwendet diese Benutzerattribute, um SAML-Assertionen (als SAML-Attribute) aufzufüllen, die an die Anwendung gesendet werden. Diese Benutzerattribute werden wiederum aus Ihrer Identitätsquelle abgerufen. Jede Anwendung bestimmt die Liste der SAML 2.0-Attribute, die sie für ein erfolgreiches Single Sign-On benötigt. 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 auf Ihrer Active Directory-Konfigurationsseite, wenn Sie Active Directory als Identitätsquelle

verwenden. Weitere Informationen finden Sie unter Zuordnung von Benutzerattributen zwischen IAM Identity Center und dem Verzeichnis Microsoft AD.

Unterstützte externe Identitätsanbieter-Attribute

In der folgenden Tabelle sind alle unterstützten Attribute des externen Identitätsanbieters (IdP) aufgeführt. Sie können Attributen zugeordnet werden, die Sie bei der Konfiguration Attribute für Zugriffskontrolle in IAM Identity Center verwenden können. Wenn Sie SAML-Assertionen verwenden, können Sie alle Attribute verwenden, die Ihr IdP unterstützt.

Unterstützte Attribute in Ihrem IdP
`${path:userName}`
`${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}`

Unterstützte Attribute in Ihrem IdP
${path:locale}
${path:timezone}
${path:enterprise.employeeNumber}
${path:enterprise.costCenter}
${path:enterprise.organization}
${path:enterprise.division}
${path:enterprise.department}
${path:enterprise.manager.value}

Standardzuordnungen zwischen IAM Identity Center und Microsoft AD

In der folgenden Tabelle sind die Standardzuordnungen für Benutzerattribute in IAM Identity Center zu den Benutzerattributen in Ihrem Verzeichnis aufgeführt. Microsoft AD IAM Identity Center unterstützt nur die Liste der Attribute in der Spalte Benutzerattribut in IAM Identity Center.

Benutzerattribut im IAM Identity Center	Ordnet diesem Attribut in Ihrem Active Directory zu
displayname	${displayname}
emails[?primary].value *	${mail}
externalid	${objectguid}
name.givenname	${givenname}
name.familyname	${sn}
name.middlename	${initials}
sid	${objectsid}

Benutzerattribut im IAM Identity Center	Ordnet diesem Attribut in Ihrem Active Directory zu
`username`	`${userprincipalname}`

* Das E-Mail-Attribut in IAM Identity Center muss innerhalb des Verzeichnisses eindeutig sein.

Gruppenattribut in IAM Identity Center	Ordnet diesem Attribut in Ihrem Active Directory zu
`externalid`	`${objectguid}`
`description`	`${description}`
`displayname`	`${samaccountname}@{associateddomain}`

Überlegungen

- Wenn Sie bei der Aktivierung der konfigurierbaren AD-Synchronisierung keine Zuweisungen für Ihre Benutzer und Gruppen in IAM Identity Center haben, werden die Standardzuordnungen in den vorherigen Tabellen verwendet. Informationen zum Anpassen dieser Zuordnungen finden Sie unter. Konfigurieren Sie Attributzuordnungen für Ihre Synchronisierung
- 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 in IAM Identity Center. Wenn Sie „username“ einem AD-Verzeichnisattribut mit einem leeren Wert zuordnen, betrachtet IAM Identity Center den `windowsUpn` Wert als Standardwert für „username“. Wenn Sie die Attributzuordnung für „Benutzername“ gegenüber Ihrer aktuellen Zuordnung ändern möchten, stellen Sie sicher, dass IAM Identity Center-Datenflüsse, die von „Benutzername“ abhängig sind, weiterhin wie erwartet funktionieren, bevor Sie die Änderung vornehmen.

Unterstützte Microsoft AD Attribute für IAM Identity Center

In der folgenden Tabelle sind alle Microsoft AD Verzeichnisattribute aufgeführt, die unterstützt werden und Benutzerattributen in IAM Identity Center zugeordnet werden können.

Unterstützte Attribute in Ihrem Microsoft AD-Verzeichnis
`${samaccountname}`
`${description}`
`${objectguid}`
`${objectsid}`
`${givenname}`
`${sn}`
`${initials}`
`${mail}`
`${userprincipalname}`
`${displayname}`
`${distinguishedname}`
`${proxyaddresses[?type == "SMTP"].value}`
`${proxyaddresses[?type == "smtp"].value}`
`${useraccountcontrol}`
`${associateddomain}`

Überlegungen

- Sie können eine beliebige Kombination unterstützter Microsoft AD Verzeichnisattribute angeben, um sie einem einzelnen veränderbaren Attribut in IAM Identity Center zuzuordnen.

Unterstützte IAM Identity Center-Attribute für Microsoft AD

In der folgenden Tabelle sind alle IAM Identity Center-Attribute aufgeführt, die unterstützt werden und Benutzerattributen in Ihrem Verzeichnis zugeordnet werden können. Microsoft AD Nachdem Sie Ihre Anwendungsattributzuordnungen eingerichtet haben, können Sie dieselben IAM Identity Center-Attribute verwenden, um sie den tatsächlichen Attributen zuzuordnen, die von dieser Anwendung verwendet werden.

Unterstützte Attribute in IAM Identity Center für Active Directory
`${user:AD_GUID}`
`${user:AD_SID}`
`${user:email}`
`${user:familyName}`
`${user:givenName}`
`${user:middleName}`
`${user:name}`
`${user:preferredUsername}`
`${user:subject}`

Zuordnung von Benutzerattributen zwischen IAM Identity Center und dem Verzeichnis Microsoft AD

Mithilfe des folgenden Verfahrens können Sie angeben, wie Ihre Benutzerattribute in IAM Identity Center den 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 Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Attribute für die Zugriffskontrolle“ und dann „Attribute verwalten“.

4. Suchen Sie auf der Seite „Attribut für Zugriffskontrolle verwalten“ in IAM Identity Center nach dem Attribut, das Sie zuordnen möchten, und geben Sie dann einen Wert in das Textfeld ein. Beispielsweise möchten Sie möglicherweise das IAM Identity Center-Benutzerattribut **`email`**dem Microsoft AD-Verzeichnisattribut zuordnen **`${mail}`**.
5. Wählen Sie Änderungen speichern aus.

IAM Identity Center, konfigurierbare AD-Synchronisierung

Mit der konfigurierbaren Active Directory-Synchronisierung (AD) von IAM Identity Center können Sie die Identitäten in Microsoft Active Directory, die automatisch mit IAM Identity Center synchronisiert werden, explizit konfigurieren und den Synchronisierungsprozess steuern.

- Mit dieser Synchronisierungsmethode können Sie Folgendes tun:
  - Kontrollieren 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. Bei den Anwendungen kann AWS es sich um verwaltete Anwendungen oder um vom Kunden verwaltete Anwendungen handeln.
  - Steuern Sie den Synchronisierungsvorgang, indem Sie die Synchronisierung bei Bedarf pausieren und wieder aufnehmen. Auf diese Weise können Sie die Auslastung der Produktionssysteme regulieren.

Voraussetzungen und Überlegungen

Bevor Sie die konfigurierbare AD-Synchronisierung verwenden, sollten Sie die folgenden Voraussetzungen und Überlegungen beachten:

- Angeben der zu synchronisierenden Benutzer und Gruppen in Active Directory

  Bevor Sie IAM Identity Center verwenden können, um neuen Benutzern und Gruppen Zugriff auf verwaltete oder vom Kunden AWS verwaltete Anwendungen zuzuweisen, müssen Sie die Benutzer und Gruppen in Active Directory angeben, die synchronisiert werden sollen, und sie dann mit IAM Identity Center synchronisieren. AWS-Konten
  - Konfigurierbare AD-Synchronisierung — IAM Identity Center durchsucht Ihren Domain-Controller nicht direkt nach Benutzern und Gruppen. Stattdessen müssen Sie zunächst die Liste der

Benutzer und Gruppen angeben, die synchronisiert werden sollen. Sie können diese Liste, auch Synchronisierungsbereich genannt, 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 mithilfe der konfigurierbaren AD-Synchronisierung zum ersten Mal synchronisieren.

- 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 bereits mit einer Liste dieser Benutzer und Gruppen gefüllt. Um neue Benutzer oder Gruppen zuzuweisen, müssen Sie sie ausdrücklich zum Synchronisierungsbereich hinzufügen. Weitere Informationen finden Sie unter Fügen Sie Benutzer und Gruppen zu Ihrem Synchronisierungsbereich hinzu.
- Neue Benutzer und Gruppen: Wenn Sie neuen Benutzern und Gruppen Zugriff auf 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 für die Zuweisung verwenden können. AWS-Konten Weitere Informationen finden Sie unter Fügen Sie Benutzer und Gruppen zu Ihrem Synchronisierungsbereich hinzu.

- Zuweisungen zu verschachtelten Gruppen in Active Directory vornehmen

  Gruppen, die Mitglieder anderer Gruppen sind, werden als verschachtelte Gruppen (oder untergeordnete Gruppen) bezeichnet.

  - Konfigurierbare AD-Synchronisierung — Die Verwendung der konfigurierbaren AD-Synchronisierung, um Zuweisungen zu einer Gruppe in Active Directory vorzunehmen, die verschachtelte Gruppen enthält, kann die Anzahl der Benutzer erhöhen, die Zugriff auf AWS-Konten oder auf Anwendungen haben. In diesem Fall gilt die Zuweisung für alle Benutzer, auch für Benutzer in verschachtelten Gruppen. Wenn Sie beispielsweise Gruppe A Zugriff zuweisen und Gruppe B Mitglied von Gruppe A ist, erben Mitglieder von Gruppe B diesen Zugriff ebenfalls.
- Aktualisierung automatisierter Workflows

  Wenn Sie automatisierte Workflows verwenden, die die IAM Identity Center-API-Aktionen für den Identitätsspeicher und die IAM Identity Center-Zuweisungs-API-Aktionen 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 anpassen, sodass sie mit konfigurierbarer AD-Synchronisierung wie erwartet funktionieren. Die konfigurierbare

AD-Synchronisierung ändert die Reihenfolge, in der Benutzer- und Gruppenzuweisungen und -bereitstellungen erfolgen, und die Art und Weise, wie Abfragen ausgeführt werden.

- Konfigurierbare AD-Synchronisierung — Die Bereitstellung erfolgt zuerst und nicht automatisch. Stattdessen müssen Sie zuerst Benutzer und Gruppen 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 unterAutomatisieren Sie Ihre Synchronisierungskonfiguration für eine konfigurierbare AD-Synchronisierung.

Themen

So funktioniert die konfigurierbare AD-Synchronisierung

IAM Identity Center aktualisiert die AD-basierten Identitätsdaten im Identitätsspeicher mithilfe des folgenden Verfahrens. Weitere Informationen zu den Voraussetzungen finden Sie unter. Voraussetzungen und Überlegungen

Erstellung

Nachdem Sie Ihr selbstverwaltetes Verzeichnis in Active Directory oder Ihr von Directory Service IAM Identity Center verwaltetes AWS Managed Microsoft AD Verzeichnis 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. Je nach Größe Ihres Verzeichnisses kann der Synchronisierungsvorgang länger dauern.

Gruppen, die Mitglieder anderer Gruppen sind (sogenannte verschachtelte Gruppen oder untergeordnete Gruppen), werden ebenfalls in den Identitätsspeicher geschrieben.

Sie können neuen Benutzern oder Gruppen erst Zugriff zuweisen, nachdem sie mit dem IAM Identity Center-Identitätsspeicher synchronisiert wurden.

Aktualisierung

Die Identitätsdaten im IAM Identity Center-Identitätsspeicher bleiben aktuell, da regelmäßig Daten aus dem Quellverzeichnis in Active Directory gelesen werden. IAM Identity Center synchronisiert standardmäßig stündlich Daten aus Ihrem Active Directory in einem Synchronisierungszyklus. Je nach Größe Ihres Active Directory kann es 30 Minuten bis 2 Stunden dauern, bis die Daten mit IAM Identity Center synchronisiert sind.

Benutzer- und Gruppenobjekte, die sich im Synchronisierungsbereich befinden, und ihre Mitgliedschaften werden in IAM Identity Center erstellt oder aktualisiert, sodass sie den entsprechenden Objekten im Quellverzeichnis in Active Directory zugeordnet werden. Bei Benutzerattributen wird nur die Teilmenge der Attribute, die im Abschnitt Attribute für die Zugriffskontrolle der IAM Identity Center-Konsole aufgeführt sind, in IAM Identity Center aktualisiert. Es kann einen Synchronisierungszyklus dauern, bis alle Attributaktualisierungen, die Sie in Active Directory vornehmen, in IAM Identity Center übernommen werden.

Sie können auch die Teilmenge der Benutzer und Gruppen aktualisieren, die Sie mit dem IAM Identity Center-Identitätsspeicher synchronisieren. Sie können wählen, ob Sie dieser Teilmenge neue Benutzer oder Gruppen hinzufügen oder sie entfernen möchten. Alle Identitäten, die Sie hinzufügen, werden bei der nächsten geplanten Synchronisierung synchronisiert. Identitäten, die Sie aus der Teilmenge entfernen, werden nicht mehr im IAM Identity Center-Identitätsspeicher 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, sofern sie nicht Teil einer anderen Gruppe sind, 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 beim nächsten Synchronisierungszyklus nicht erneut mit IAM Identity Center synchronisiert werden.

Sie können die Synchronisation auch jederzeit unterbrechen und neu starten. Wenn Sie die Synchronisation für mehr als 28 Tage unterbrechen, werden alle Ihre Benutzer deaktiviert.

Konfigurieren Sie Attributzuordnungen für Ihre Synchronisierung

Weitere Informationen zu verfügbaren Attributen finden Sie unter. Attributzuordnungen zwischen dem IAM Identity Center und dem Verzeichnis externer Identitätsanbieter

So konfigurieren Sie Attributzuordnungen in IAM Identity Center zu Ihrem Verzeichnis

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“, dann „Aktionen“ und anschließend „Synchronisation verwalten“.
4. Wählen Sie unter Synchronisation verwalten die Option Attributzuordnung anzeigen aus.
5. Konfigurieren Sie unter Active Directory-Benutzerattribute die IAM Identity Center-Identitätsspeicherattribute und die Active Directory-Benutzerattribute. Beispielsweise möchten Sie möglicherweise das IAM Identity Center-Identitätsspeicherattribut `email` dem Active Directory-Benutzerverzeichnisattribut zuordnen. `${objectguid}`

   > **Note**
   >
   > Unter Gruppenattribute können die IAM Identity Center-Identitätsspeicherattribute und die Active Directory-Gruppenattribute nicht geändert werden.

6. Wählen Sie Änderungen speichern aus. Dadurch kehren Sie zur Seite „Sync verwalten“ zurück.

Einrichtung der erstmaligen Synchronisierung von Active Directory mit IAM Identity Center

Gehen Sie wie folgt vor, wenn Sie Ihre Benutzer und Gruppen zum ersten Mal aus Active Directory mit dem IAM Identity Center synchronisieren. Alternativ können Sie den unter beschriebenen Schritten folgen, Ändern Sie Ihre Identitätsquelle um Ihre Identitätsquelle von IAM Identity Center auf Active Directory zu ändern.

Geführte Einrichtung

1. Öffnen Sie die IAM-Identity-Center-Konsole.

> **Note**
>
> Stellen Sie sicher, dass die IAM Identity Center-Konsole eines der Verzeichnisse verwendet, AWS-Regionen in dem sich Ihr AWS Managed Microsoft AD Verzeichnis befindet, bevor Sie mit dem nächsten Schritt fortfahren.

2. Wählen Sie Einstellungen aus.
3. Wählen Sie oben auf der Seite in der Benachrichtigung die Option Geführte Installation starten aus.
4. Überprüfen Sie in Schritt 1 — optional: Attributzuordnungen konfigurieren die standardmäßigen Benutzer- und Gruppenattributzuordnungen. Wenn keine Änderungen erforderlich sind, wählen Sie Weiter. Wenn Änderungen erforderlich sind, nehmen Sie die Änderungen vor und wählen Sie dann Änderungen speichern.
5. Wählen Sie in Schritt 2 — optional: Synchronisierungsbereich konfigurieren die Registerkarte Benutzer aus. Geben Sie dann den genauen Benutzernamen des Benutzers ein, den Sie zu Ihrem Synchronisierungsbereich hinzufügen möchten, und wählen Sie Hinzufügen. Wählen Sie als Nächstes die Registerkarte Gruppen. Geben Sie den genauen Gruppennamen der Gruppe ein, die Sie zu Ihrem Synchronisierungsbereich hinzufügen möchten, und wählen Sie Hinzufügen. Klicken Sie anschließend auf Next (Weiter). Wenn Sie später Benutzer und Gruppen zu Ihrem Synchronisierungsbereich hinzufügen möchten, nehmen Sie keine Änderungen vor und wählen Sie Weiter.
6. Bestätigen Sie in Schritt 3: Konfiguration überprüfen und speichern Sie 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“.

Fügen Sie Benutzer und Gruppen zu Ihrem Synchronisierungsbereich hinzu

Fügen Sie Ihre Active Directory-Benutzer und -Gruppen zu IAM Identity Center hinzu, indem Sie die folgenden Schritte ausführen.

So fügen Sie Benutzer hinzu

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie 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. Überprüfen Sie unter Hinzugefügte Benutzer und Gruppen den Benutzer, den Sie hinzufügen möchten.
7. Wählen Sie Absenden aus.
8. Klicken Sie im Navigationsbereich auf Users (Benutzer). Wenn der von Ihnen angegebene Benutzer nicht in der Liste angezeigt wird, wählen Sie das Aktualisierungssymbol, um die Benutzerliste zu aktualisieren.

Um Gruppen hinzuzufügen

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“, dann „Aktionen“ und anschließend „Synchronisation verwalten“ aus.
4. Wählen Sie auf der Seite „Synchronisation verwalten“ den Tab 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 Hinzugefügte Benutzer und Gruppen die Gruppe, die Sie hinzufügen möchten.
7. Wählen Sie Absenden aus.
8. Wählen Sie im Navigationsbereich die Option Groups (Gruppen). Wenn die von Ihnen angegebene Gruppe nicht in der Liste angezeigt wird, wählen Sie das Aktualisierungssymbol, um die Gruppenliste zu aktualisieren.

Entfernen Sie Benutzer und Gruppen aus Ihrem Synchronisierungsbereich

Weitere Informationen darüber, was passiert, wenn Sie Benutzer und Gruppen aus Ihrem Synchronisierungsbereich entfernen, finden Sie unterSo funktioniert die konfigurierbare AD-Synchronisierung.

Um Benutzer zu entfernen

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“, dann „Aktionen“ und anschließend „Synchronisation 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.

Um Gruppen zu entfernen

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“, dann „Aktionen“ und anschließend „Synchronisation 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.

Unterbrechen Sie die Synchronisierung und setzen Sie sie fort

Wenn Sie Ihre Synchronisierung unterbrechen, werden alle future Synchronisierungszyklen angehalten und verhindert, dass Änderungen, die Sie an Benutzern und Gruppen in Active Directory vornehmen, in IAM Identity Center widergespiegelt werden. Nachdem Sie die Synchronisierung

wieder aufgenommen haben, übernimmt der Synchronisierungszyklus diese Änderungen ab der nächsten geplanten Synchronisierung.

Um die Synchronisierung anzuhalten

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ den Tab „Identitätsquelle“, dann „Aktionen“ und anschließend „Synchronisation verwalten“ aus.
4. Wählen Sie unter „Synchronisierung verwalten“ die Option „Synchronisierung unterbrechen“ aus.

Um die Synchronisierung fortzusetzen

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ den Tab „Identitätsquelle“, dann „Aktionen“ und anschließend „Synchronisation verwalten“ aus.
4. Wählen Sie unter Synchronisierung verwalten die Option Synchronisierung fortsetzen aus.

> **Note**
>
> Wenn Sie „Synchronisierung unterbrechen“ statt „Synchronisierung fortsetzen“ sehen, wurde die Synchronisierung von Active Directory mit IAM Identity Center bereits wieder aufgenommen.

Automatisieren Sie Ihre Synchronisierungskonfiguration für eine konfigurierbare AD-Synchronisierung

Um sicherzustellen, dass Ihr automatisierter Workflow mit konfigurierbarer AD-Synchronisierung wie erwartet funktioniert, empfehlen wir Ihnen, die folgenden Schritte durchzuführen, um Ihre Synchronisierungskonfiguration zu automatisieren.

Um Ihre Synchronisierungskonfiguration für die konfigurierbare AD-Synchronisierung zu automatisieren

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 der Gruppe IAMIdentityCenterAllUsersAndGroupsbeispielsweise einen Namen geben.
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.

Benutzer im Identity Center-Verzeichnis 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 stehen sofort für die Zuweisung von Aufgaben und für Anwendungen zur Verfügung. Weitere Informationen finden Sie unter Bereitstellung von Benutzern und Gruppen.

Ändern Sie Ihre Identitätsquelle

Wenn Sie Benutzer lieber in verwalten möchten 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 Sie Directory Service Weitere

Informationen finden Sie unter Überlegungen zuWechseln zwischen dem IAM Identity Center-Verzeichnis 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. Wechsel von IAM Identity Center zu einem externen IdP

Themen

Fügen Sie Benutzer zu Ihrem Identity Center-Verzeichnis hinzu

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 zu Ihrem Identity Center-Verzeichnis hinzuzufügen. Alternativ können Sie den AWS API-Vorgang aufrufen CreateUser, um Benutzer hinzuzufügen.

Console

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. Es 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. Eine E-Mail mit Anweisungen zur Passworteinrichtung an diesen Benutzer senden — Diese Option sendet dem Benutzer automatisch eine von Amazon Web Services adressierte E-Mail mit der Betreffzeile Einladung zum Beitritt AWS IAM Identity Center. In der E-Mail wird der Benutzer im Namen Ihres Unternehmens aufgefordert, auf das Zugriffsportal für das IAM Identity Center AWS zuzugreifen, und es wird ein Passwort registriert. Die E-Mail-Einladung läuft in sieben Tagen ab. In diesem Fall können Sie die E-Mail erneut senden, indem Sie „Passwort zurücksetzen“ und dann „E-Mail an den Benutzer senden“ mit Anweisungen zum Zurücksetzen des Passworts auswählen. Bevor der Benutzer die Einladung annimmt, wird der Link E-Mail-Bestätigung senden angezeigt, mit dem die E-Mail-Adresse bestätigt werden soll. Dieser Schritt ist jedoch optional und verschwindet, nachdem der Benutzer die Einladung angenommen und ein Passwort registriert hat.

      > **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 E-Mails mit Amazon SES.
      > Alle vom IAM Identity Center-Dienst gesendeten E-Mails stammen entweder von der Adresse `no-reply@signin.aws.com` oder `no-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 Einmalkennwort, das Sie mit diesem Benutzer teilen können — Mit dieser Option erhalten Sie die URL und das Passwort des AWS Zugriffsportals, die Sie dem Benutzer manuell von Ihrer E-Mail-Adresse aus senden können. Der Benutzer muss seine E-Mail-Adresse verifizieren. Sie können den Vorgang einleiten, indem Sie auf Link zur E-Mail-Bestätigung senden klicken. Der Link zur E-Mail-Bestätigung läuft in sieben Tagen ab. In diesem Fall können Sie den Link zur E-

Mail-Bestätigung erneut senden, indem Sie Passwort zurücksetzen und dann Einmalpasswort generieren und das Passwort mit dem Benutzer teilen wählen.

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 Stellen Sie Benutzer und Gruppen von einem externen Identitätsanbieter mithilfe von SCIM bereit.

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 aus.

AWS CLI

So fügen Sie einen Benutzer hinzu

Der folgende `create-user` Befehl erstellt einen neuen Benutzer in Ihrem Identity Center-Verzeichnis.

```
aws identitystore create-user \
    --identity-store-id d-1234567890 \
    --user-name johndoe \
    --name "GivenName=John,FamilyName=Doe" \
```

```
    --display-name "John Doe" \
    --emails "Type=work,Value=johndoe@example.com"
```

Ausgabe:

```
{
    "UserId": "1234567890-abcdef",
    "IdentityStoreId": "d-1234567890"
}
```

> **Note**
>
> Wenn Sie Benutzer mit dem `create-user` CLI-Befehl oder der CreateUserAPI-Operation erstellen, haben die Benutzer keine Passwörter. Sie können die Einstellungen in IAM Identity Center aktualisieren, um diesen Benutzern nach ihrem ersten Anmeldeversuch eine Bestätigungs-E-Mail zu senden, damit sie ein Passwort einrichten können. Wenn Sie diese Einstellung nicht aktivieren, müssen Sie ein Einmalkennwort generieren und es mit dem Benutzer teilen. Weitere Informationen finden Sie unter Einmalpasswort per E-Mail an Benutzer senden, die mit API oder CLI erstellt wurden.

Fügen Sie Gruppen zu Ihrem Identity Center-Verzeichnis hinzu

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

Console

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 Aufschluss über die Berechtigungen geben, die 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.

AWS CLI

So fügen Sie eine Gruppe hinzu

Der folgende `create-group` Befehl erstellt eine neue Gruppe in Ihrem Identity Center-Verzeichnis.

```
aws identitystore create-group \
    --identity-store-id d-1234567890 \
    --display-name "Developers" \
    --description "Group that contains all developers"
```

Ausgabe:

```
{
    "GroupId": "1a2b3c4d-5e6f-7g8h-9i0j-1k2l3m4n5o6p",
    "IdentityStoreId": "d-1234567890"
}
```

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

Fügen Sie Benutzer zu Gruppen hinzu

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

Console

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).

AWS CLI

So fügen Sie einen Benutzer einer Gruppe als Mitglied hinzu

Mit dem folgenden `create-group-membership` Befehl wird einer Gruppe in Ihrem Identity Center-Verzeichnis ein Benutzer hinzugefügt.

```
aws identitystore create-group-membership \
    --identity-store-id d-1234567890 \
    --group-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222 \
    --member-id UserId=a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Ausgabe:

```
{
    "MembershipId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
    "IdentityStoreId": "d-1234567890"
}
```

Löschen Sie Gruppen in 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 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

Console

So löschen Sie eine Gruppe

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“.

AWS CLI

So löschen Sie eine Gruppe

Der folgende `delete-group` Befehl löscht die angegebene Gruppe aus Ihrem Identity Center-Verzeichnis.

```
aws identitystore delete-group \
    --identity-store-id d-1234567890 \
    --group-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222
```

Benutzer in IAM Identity Center löschen

Wenn Sie einen Benutzer in Ihrem IAM Identity Center-Verzeichnis löschen, wird ihm dadurch der Zugriff auf AWS-Konten und die Anwendungen entzogen. Nachdem Sie einen Benutzer gelöscht haben, können Sie diese Aktion nicht rückgängig machen. Gehen Sie wie folgt vor, um einen Benutzer in Ihrem Identity Center-Verzeichnis 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 Grundlegendes zu Authentifizierungssitzungen in IAM Identity Center.

> **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

Console

Benutzer löschen

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.

AWS CLI

Benutzer löschen

Der folgende `delete-user` Befehl löscht einen Benutzer aus Ihrem Identity Center-Verzeichnis.

```
aws identitystore delete-user \
    --identity-store-id d-1234567890 \
    --user-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Benutzer aus Gruppen entfernen

Gehen Sie wie folgt vor, um Mitglieder aus einer Gruppe zu entfernen. Alternativ können Sie den AWS API-Vorgang aufrufen DeleteGroupMembership, um einen Benutzer aus einer Gruppe zu entfernen.

Console

Um einen Benutzer aus einer Gruppe zu entfernen

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Klicken Sie auf Groups (Gruppen).
3. Wählen Sie die Gruppe aus, die Sie aktualisieren möchten.
4. Wählen Sie auf der Seite mit den Gruppendetails unter Benutzer in dieser Gruppe die Benutzer aus, die Sie entfernen möchten.
5. Wählen Sie Benutzer aus Gruppe entfernen aus.
6. Wählen Sie im Dialogfeld Benutzer entfernen die Option Benutzer aus Gruppe entfernen aus, um zu überprüfen, ob Sie den Benutzern den Zugriff auf das Konto und die Anwendungen, die der Gruppe zugewiesen sind, entziehen möchten.

AWS CLI

Um einen Benutzer aus einer Gruppe zu entfernen

Mit dem folgenden `delete-group-membership` Befehl wird eine Mitgliedschaft aus einer Gruppe entfernt.

```
aws identitystore delete-group-membership
    --identity-store-id d-1234567890 \
    --membership-id a1b2c3d4-5678-90ab-cdef-EXAMPLE33333
```

Benutzereigenschaften des Identity Center-Verzeichnisses bearbeiten

Gehen Sie wie folgt vor, um die Eigenschaften eines Benutzers in Ihrem Identity Center-Verzeichnis zu bearbeiten. Alternativ können Sie den AWS API-Vorgang aufrufen, UpdateUserum die Benutzereigenschaften zu aktualisieren.

Console

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. Wählen Sie dann 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.

AWS CLI

Um Benutzereigenschaften im IAM Identity Center zu bearbeiten

Mit dem folgenden `update-user` Befehl wird der Spitzname des Benutzers aktualisiert.

```
aws identitystore update-user \
    --identity-store-id d-1234567890 \
    --user-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --operations '{"AttributePath":"nickName","AttributeValue":"Johnny"}'
```

Richten Sie den Zugriff der Belegschaft auf AWS Ressourcen ein

Richten Sie ein, wie sich die Benutzer Ihrer Belegschaft über IAM Identity Center authentifizieren und auf AWS Ressourcen zugreifen. In diesem Abschnitt werden die folgenden Komponenten behandelt, die den Benutzerzugriff Ihrer Mitarbeiter auf Ihre AWS Umgebung regeln:

- Authentifizierungssitzungen — Erfahren Sie, wie IAM Identity Center verschiedene Arten von Benutzersitzungen verwaltet, von interaktiven Portalsitzungen bis hin zu Anwendungssitzungen im Hintergrund, und wie diese miteinander interagieren.
- Verwaltung des Benutzerzugriffs — Konfigurieren Sie die Sitzungsdauer, deaktivieren Sie Benutzerkonten und implementieren Sie unternehmensweite Zugriffssperren, um Sicherheit und Compliance zu gewährleisten.
- Passwortverwaltung — Legen Sie für Benutzer, die im Identity Center-Verzeichnis erstellt wurden, Kennwortanforderungen fest, kümmern Sie sich um die Einrichtung der Benutzeranmeldedaten und verwalten Sie das Zurücksetzen von Passwörtern für Benutzer.
- Multi-Faktor-Authentifizierung — Verbessern Sie für Benutzer, die im Identity Center-Verzeichnis erstellt wurden, die Sicherheit mit MFA, indem Sie Authentifikator-Apps, Sicherheitsschlüssel oder integrierte Authentifikatoren verwenden, um Benutzeranmeldungen zu schützen.

Themen

Grundlegendes zu Authentifizierungssitzungen in IAM Identity Center

Wenn sich ein Benutzer beim AWS Zugriffsportal anmeldet, erstellt IAM Identity Center eine Authentifizierungssitzung, die die verifizierte Identität des Benutzers darstellt.

Nach der Authentifizierung kann der Benutzer ohne zusätzliche Anmeldungen auf alle ihm zugewiesenen AWS-Konten, AWS verwalteten Anwendungen sowie auf vom Kunden verwaltete Anwendungen zugreifen, zu deren Verwendung ihm Administratoren eine Nutzungsberechtigung erteilt haben.

Arten von Authentifizierungssitzungen

Interaktive Benutzersitzungen

Nachdem sich ein Benutzer beim AWS Zugriffsportal angemeldet hat, erstellt IAM Identity Center eine interaktive Benutzersitzung. Diese Sitzung stellt den authentifizierten Status des Benutzers innerhalb von IAM Identity Center dar und dient als Grundlage für die Erstellung anderer Sitzungstypen. Interaktive Benutzersitzungen können für die in IAM Identity Center konfigurierte Dauer dauern, die bis zu 90 Tage betragen kann.

Interaktive Benutzersitzungen sind der primäre Authentifizierungsmechanismus. Sie enden, wenn sich der Benutzer abmeldet oder wenn ein Administrator seine Sitzung beendet. Die Dauer dieser Sitzungen sollte sorgfältig auf der Grundlage der Sicherheitsanforderungen Ihres Unternehmens konfiguriert werden.

Hinweise zur Konfiguration der Dauer interaktiver Benutzersitzungen finden Sie unterthe section called “Konfigurieren Sie die Sitzungsdauer”.

Anwendungssitzungen

Anwendungssitzungen sind authentifizierte Verbindungen zwischen Benutzern und AWS verwalteten Anwendungen (wie Amazon Q Developer oder Amazon Quick Suite), die IAM Identity Center über Single Sign-On herstellt.

Standardmäßig haben Anwendungssitzungen eine Lebensdauer von einer Stunde, sie werden jedoch automatisch aktualisiert, solange die zugrunde liegende interaktive Benutzersitzung gültig bleibt. Dieser Aktualisierungsmechanismus bietet Benutzern ein nahtloses Benutzererlebnis und gewährleistet gleichzeitig die Einhaltung der Sicherheitskontrollen. Wenn eine interaktive Benutzersitzung entweder durch Abmeldung des Benutzers oder durch eine Administratoraktion beendet wird, werden die Anwendungssitzungen beim nächsten Aktualisierungsversuch beendet, normalerweise innerhalb von 30 Minuten.

Hintergrundsitzungen für Benutzer

Benutzerhintergrundsitzungen sind Sitzungen mit längerer Dauer, die für Anwendungen konzipiert sind, bei denen Prozesse stunden- oder tagelang ohne Unterbrechung ausgeführt werden müssen. Derzeit gilt dieser Sitzungstyp hauptsächlich für Amazon SageMaker Studio, wo Datenwissenschaftler möglicherweise Schulungsaufgaben für maschinelles Lernen ausführen, deren Bearbeitung viele Stunden in Anspruch nimmt.

Informationen zur Konfiguration der Dauer von Benutzerhintergrundsitzungen finden Sie unter Benutzerhintergrundsitzungen.

Amazon Q Entwicklersitzungen

Sie können Amazon Q Developer-Sitzungen verlängern, sodass Entwickler, die Amazon Q Developer verwenden IDEs , die Authentifizierung für bis zu 90 Tage aufrechterhalten können. Diese Funktion reduziert Anmeldeunterbrechungen, während Sie an Code arbeiten.

Diese Sitzungen sind unabhängig von anderen Sitzungstypen und wirken sich nicht auf benutzerinteraktive Sitzungen oder andere AWS verwaltete Anwendungen aus. Je nachdem, wann Sie IAM Identity Center aktiviert haben, ist diese Funktion möglicherweise standardmäßig aktiviert.

Informationen zur Konfiguration erweiterter Amazon Q Developer-Sitzungen finden Sie unter???.

Von IAM Identity Center erstellte IAM-Rollensitzungen

IAM Identity Center erstellt einen anderen Sitzungstyp, wenn Benutzer auf das oder zugreifen. AWS-Managementkonsole AWS CLI In diesen Fällen verwendet IAM Identity Center die Anmeldesitzung, um eine IAM-Sitzung aufzurufen, indem es eine IAM-Rolle annimmt, die im Berechtigungssatz des Benutzers angegeben ist.

> **Important**
>
> Im Gegensatz zu Anwendungssitzungen funktionieren IAM-Rollensitzungen unabhängig voneinander, sobald sie eingerichtet wurden. Sie bleiben für die im Berechtigungssatz konfigurierte Dauer bestehen, die unabhängig vom Status der ursprünglichen Anmeldesitzung bis zu 12 Stunden betragen kann. Dieses Verhalten stellt sicher, dass lang andauernde CLI-Operationen oder Konsolensitzungen nicht unerwartet beendet werden.

Möglichkeiten, Benutzersitzungen im IAM Identity Center zu beenden

Vom Benutzer initiiert

Wenn sich ein Benutzer vom AWS Zugriffsportal abmeldet, wird die Anmeldesitzung beendet, sodass der Benutzer nicht mehr auf neue Ressourcen zugreifen kann.

Bestehende Anwendungssitzungen werden jedoch nicht sofort beendet. Stattdessen enden sie innerhalb von etwa 30 Minuten, wenn sie bei der nächsten Aktualisierung feststellen, dass die Anmeldesitzung nicht mehr gültig ist. Bestehende IAM-Rollensitzungen werden fortgesetzt, bis sie je nach Konfiguration des Berechtigungssatzes ablaufen, was bis zu 12 Stunden später sein kann.

Vom Administrator initiiert

Jeder Benutzer mit Administratorberechtigungen für IAM Identity Center in Ihrer Organisation, in der Regel IT-Administratoren oder Sicherheitsteams, kann die Sitzung eines Benutzers beenden. Diese Aktion funktioniert genauso, als ob sich Benutzer selbst abmelden würden, sodass Administratoren verlangen können, dass sich Benutzer bei Bedarf erneut anmelden. Diese Funktion ist nützlich, wenn sich Sicherheitsrichtlinien ändern oder wenn verdächtige Aktivitäten erkannt werden.

Wenn ein IAM Identity Center-Administrator einen Benutzer löscht oder den Zugriff eines Benutzers deaktiviert, verliert der Benutzer den Zugriff auf das AWS Zugriffsportal und kann sich nicht erneut anmelden, um eine neue Anwendung oder IAM-Rollensitzung zu starten. Der Benutzer verliert innerhalb von 30 Minuten den Zugriff auf bestehende Anwendungssitzungen. Alle bestehenden IAM-Rollensitzungen werden auf der Grundlage der Sitzungsdauer fortgesetzt, die im IAM Identity Center-Berechtigungssatz konfiguriert ist. Die maximale Sitzungsdauer kann 12 Stunden betragen.

Was passiert mit dem Benutzerzugriff, wenn Sie eine Sitzung beenden

Diese Referenz enthält detaillierte Informationen darüber, wie sich IAM Identity Center-Sitzungen verhalten, wenn administrative Maßnahmen ergriffen werden. Die Tabellen in diesem Abschnitt zeigen die Dauer und die Auswirkungen von Benutzerverwaltungsaktionen und Berechtigungsänderungen auf den Zugriff auf das AWS Zugriffsportal, Anwendungen und AWS-Konto Sitzungen.

Benutzerverwaltung

In dieser Tabelle wird zusammengefasst, wie sich Änderungen der Benutzerverwaltung auf den Zugriff auf AWS Ressourcen, Anwendungssitzungen und AWS Kontositzungen auswirken.

Action	Der Benutzer verliert den Zugriff auf das IAM Identity Center	Der Benutzer kann keine neuen Anwendungssitzungen erstellen	Der Benutzer kann nicht auf bestehende Anwendungssitzungen zugreifen	Der Benutzer verliert den Zugriff auf bestehende AWS-Konto Sitzungen
Benutzerzugriff deaktiviert	Mit sofortiger Wirkung	Mit sofortiger Wirkung	Innerhalb von 30 Minuten	Innerhalb von 12 Stunden oder weniger. Die Dauer hängt von der für den Berechtigungssatz konfigurierten Ablaufdauer der IAM-Rollensitzung ab.
Der Benutzer wurde gelöscht	Mit sofortiger Wirkung	Mit sofortiger Wirkung	Innerhalb von 30 Minuten	Innerhalb von 12 Stunden oder weniger. Die Dauer hängt von der für den Berechtigungssatz konfigurierten Ablaufdauer der IAM-Rollensitzung ab.
Benutzersitzung wurde aufgehoben	Der Benutzer muss sich erneut anmelden, um wieder Zugriff zu erhalten	Mit sofortiger Wirkung	Innerhalb von 30 Minuten	Innerhalb von 12 Stunden oder weniger. Die Dauer hängt von der für den Berechtig

Action	Der Benutzer verliert den Zugriff auf das IAM Identity Center	Der Benutzer kann keine neuen Anwendung ssitzungen erstellen	Der Benutzer kann nicht auf bestehende Anwendung ssitzungen zugreifen	Der Benutzer verliert den Zugriff auf bestehende AWS-Konto Sitzungen
				ungssatz konfigurierten Ablaufdauer der IAM-Rolle nsitzung ab.
Der Benutzer meldet sich ab	Der Benutzer muss sich erneut anmelden, um wieder Zugriff zu erhalten	Mit sofortiger Wirkung	Innerhalb von 30 Minuten	Innerhalb von 12 Stunden oder weniger. Die Dauer hängt von der für den Berechtig ungssatz konfigurierten Ablaufdauer der IAM-Rolle nsitzung ab.

Gruppenmitgliedschaft

In dieser Tabelle wird zusammengefasst, wie sich Änderungen an Benutzerberechtigungen und Gruppenmitgliedschaften auf den Zugriff auf AWS Ressourcen, Anwendungssitzungen und AWS Kontositzungen auswirken.

Action	Der Benutzer verliert den Zugriff auf das IAM Identity Center	Der Benutzer kann keine neuen Anwendungssitzungen erstellen	Der Benutzer kann nicht auf bestehende Anwendungssitzungen zugreifen	Der Benutzer verliert den Zugriff auf bestehende AWS-Konto Sitzungen
Die Anwendung oder der AWS-Konto Zugriff wurde dem Benutzer entzogen	Nein — Der Benutzer kann weiterhin auf IAM Identity Center zugreifen	Mit sofortiger Wirkung	Innerhalb von 1 Stunde	Innerhalb von 12 Stunden oder weniger. Die Dauer hängt von der für den Berechtigungssatz konfigurierten Ablaufdauer der IAM-Rollensitzung ab.
Der Benutzer wurde aus der Gruppe entfernt, der eine Anwendung zugewiesen war, oder AWS-Konto	Nein — Der Benutzer kann weiterhin auf IAM Identity Center zugreifen	Innerhalb von 1 Stunde	Innerhalb von 2 Stunden	Innerhalb von 12 Stunden oder weniger. Die Dauer hängt von der für den Berechtigungssatz konfigurierten Ablaufdauer der IAM-Rollensitzung ab.
Die Anwendung oder der AWS-Konto Zugriff wurde aus der Gruppe entfernt	Nein — Der Benutzer kann weiterhin auf IAM Identity Center zugreifen	Mit sofortiger Wirkung	Innerhalb von 1 Stunde	Innerhalb von 12 Stunden oder weniger. Die Dauer hängt von der für den Berechtig

Action	Der Benutzer verliert den Zugriff auf das IAM Identity Center	Der Benutzer kann keine neuen Anwendungssitzungen erstellen	Der Benutzer kann nicht auf bestehende Anwendungssitzungen zugreifen	Der Benutzer verliert den Zugriff auf bestehende AWS-Konto Sitzungen
				ungssatz konfigurierten Ablaufdauer der IAM-Rollensitzung ab.

> **Note**
>
> Das AWS Zugriffsportal und spiegelt AWS CLI die aktualisierten Benutzerberechtigungen innerhalb von 1 Stunde wider, nachdem Sie einen Benutzer zu dieser Gruppe hinzugefügt oder aus dieser entfernt haben.

Verstehen von Zeitunterschieden

- Sofort wirksam — Aktionen, die eine sofortige erneute Authentifizierung erfordern.
- Innerhalb von 30 Minuten bis 2 Stunden benötigen Anwendungssitzungen Zeit, um beim IAM Identity Center nachzufragen und etwaige Änderungen zu ermitteln.
- Innerhalb von 12 Stunden oder weniger — IAM-Rollensitzungen werden unabhängig voneinander ausgeführt und enden erst, wenn ihre konfigurierte Dauer abgelaufen ist.

Einmaliges Abmelden

IAM Identity Center unterstützt kein SAML Single Logout (ein Protokoll, das Benutzer automatisch von allen verbundenen Anwendungen abmeldet, wenn sie sich von einer abmelden), das von einem Identitätsanbieter initiiert wurde, der als Ihre Identitätsquelle fungiert. Darüber hinaus sendet es SAML Single Logout nicht an SAML 2.0-Anwendungen, die IAM Identity Center als Identitätsanbieter verwenden.

Bewährte Methoden für die Sitzungsverwaltung

Effektives Sitzungsmanagement erfordert eine durchdachte Konfiguration und Überwachung. Organizations sollten die Sitzungsdauer entsprechend ihren Sicherheitsanforderungen konfigurieren und generell kürzere Zeiträume für sensible Anwendungen und Umgebungen verwenden.

Die Implementierung von Prozessen zum Beenden von Sitzungen, wenn Benutzer die Rollen wechseln oder das Unternehmen verlassen, ist für die Einhaltung der Sicherheitsgrenzen unerlässlich. Die regelmäßige Überprüfung der aktiven Sitzungen sollte in die Sicherheitsüberwachung integriert werden, um ungewöhnliches Verhalten zu erkennen, das auf Sicherheitsprobleme hinweisen könnte, wie z. B. ungewöhnliche Zugriffsmuster, unerwartete Anmeldezeiten oder -orte oder Zugriff auf Ressourcen außerhalb der normalen Arbeitsfunktionen.

Konfigurieren Sie die Sitzungsdauer im IAM Identity Center

Sie können die Sitzungsdauer für Ihre Workforce-Benutzer konfigurieren, wenn sie die AWS-Zugangsportal und Anwendungen verwenden, die mit IAM Identity Center funktionieren, einschließlich Amazon Q Developer. IAM Identity Center bietet die folgenden Sitzungstypen: interaktive Benutzersitzungen, Benutzersitzungen im Hintergrund und erweiterte Sitzungen für Amazon Q Developer.

Themen

Interaktive Benutzersitzungen

Interaktive Benutzersitzungen sind Sitzungen, die an die Anmeldung eines Benutzers am AWS Zugriffsportal oder den Zugriff auf AWS verwaltete Anwendungen gebunden sind. Die Sitzungsdauer der Authentifizierung bei den Anwendungen AWS-Zugangsportal und ist die maximale Dauer, für die ein Benutzer angemeldet werden kann, ohne sich erneut zu authentifizieren. Wenn Sie eine

aktive AWS Access-Portal-Sitzung beenden, werden damit auch alle Sitzungen für diese verwalteten Anwendungen beendet.

Die Standardsitzungsdauer für interaktive Benutzersitzungen beträgt 8 Stunden. Sie können eine andere Dauer angeben, von mindestens 15 Minuten bis maximal 90 Tagen. Benutzerdefinierte Werte für die Dauer müssen in Minuten eingegeben werden und zwischen 15 Minuten und 129.600 Minuten (90 Tage) liegen. Weitere Informationen finden Sie unter Grundlegendes zu Authentifizierungssitzungen in IAM Identity Center.

Um die Dauer einer interaktiven Benutzersitzung zu konfigurieren

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Authentifizierung aus.
4. Wählen Sie unter Authentifizierung neben Sitzungsdauer die Option Konfigurieren aus. Das Dialogfeld Sitzungsdauer konfigurieren wird angezeigt.
5. Wählen Sie im Dialogfeld Sitzungsdauer konfigurieren unter Benutzerinteraktive Sitzungen die maximale Sitzungsdauer für Ihre Benutzer aus, indem Sie den Dropdown-Pfeil auswählen. Wählen Sie die Länge für die Sitzung aus und klicken Sie dann auf Speichern.

   > **Note**
   >
   > Änderungen der Sitzungsdauer gelten nur für neue Sitzungen. Aktuelle Sitzungen behalten ihre ursprüngliche Dauer bei.

6. Sie kehren zur Registerkarte Authentifizierung zurück. Über der Registerkarte wird eine grüne Benachrichtigung angezeigt, die darauf hinweist, dass die Sitzungseinstellungen erfolgreich aktualisiert wurden.

Hintergrundsitzungen der Benutzer

Benutzerhintergrundsitzungen ermöglichen es einem Benutzer, einen Job mit langer Laufzeit in einer AWS verwalteten Anwendung wie Amazon SageMaker Studio zu initiieren, ohne dass dieser Benutzer angemeldet bleiben muss, während der Job ausgeführt wird. Der Job wird sofort ausgeführt und nutzt die Trusted Identity Propagation-Funktion von IAM Identity Center, um sicherzustellen, dass die Benutzerberechtigungen erhalten bleiben, während der Job im Hintergrund ausgeführt wird. Der Job kann auch dann weiter ausgeführt werden, wenn der Benutzer seinen Computer ausschaltet,

seine IAM Identity Center-Anmeldesitzung abläuft oder sich der Benutzer vom Access Portal abmeldet. AWS Diese Funktion ermöglicht es Datenwissenschaftlern, Ingenieuren für maschinelles Lernen und anderen, Analysen und maschinelles Lernen zu starten, die im Hintergrund ohne aktive Benutzerbeteiligung ausgeführt werden.

Benutzerhintergrundsitzungen sind standardmäßig für unterstützte AWS verwaltete Anwendungen wie Amazon SageMaker Studio aktiviert. Um diese Funktion nutzen zu können, müssen Sie jedoch die Verbreitung vertrauenswürdiger Identitäten in Amazon SageMaker Studio aktivieren, wenn Sie eine Domain erstellen oder aktualisieren. Weitere Informationen finden Sie unter Aktivieren der Verbreitung vertrauenswürdiger Identitäten in Ihrer Amazon SageMaker AI-Domain.

Die Standardsitzungsdauer für Benutzersitzungen im Hintergrund beträgt 7 Tage. Sie können eine andere Dauer angeben, von mindestens 15 Minuten bis maximal 90 Tagen. Benutzerdefinierte Werte für die Dauer müssen in Minuten eingegeben werden und zwischen 15 Minuten und 129.600 Minuten (90 Tage) liegen.

Beachten Sie bei Hintergrundsitzungen für Benutzer die folgenden Überlegungen:

- Eine Benutzerhintergrundsitzung kann nur erstellt werden, wenn ein Benutzer manuell einen Job in Amazon SageMaker Studio initiiert. Diese Funktion wird für automatisierte, geplante Workflows nicht unterstützt.
- Eine Liste der AWS Regionen, die Hintergrundsitzungen von Benutzern unterstützen, finden Sie unter Unterstützte AWS Regionen.
- Sie können Hintergrundsitzungen von Benutzern in anzeigen CloudTrail. Weitere Informationen finden Sie unter Identifizieren von Sitzungsdetails im Hintergrund von Benutzern.
- Sie können auch aktive Sitzungen für einen Benutzer in Ihrer Organisation beenden. Weitere Informationen finden Sie unter Beenden aktiver Sitzungen für Ihre Workforce-Benutzer.

So konfigurieren Sie die Dauer einer Benutzersitzung im Hintergrund

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Authentifizierung aus.
4. Wählen Sie unter Authentifizierung neben Sitzungsdauer die Option Konfigurieren aus. Das Dialogfeld Sitzungsdauer konfigurieren wird angezeigt.

5. Wenn im Dialogfeld Sitzungsdauer konfigurieren das Kontrollkästchen Benutzerhintergrundsitzungen aktivieren noch nicht aktiviert ist, wählen Sie es aus. Deaktivieren Sie das Kontrollkästchen, um Benutzerhintergrundsitzungen zu deaktivieren.

   > **Note**
   >
   > Aktuelle Sitzungen sind nicht betroffen, wenn Sie Benutzerhintergrundsitzungen deaktivieren.

6. Wählen Sie unter Benutzerhintergrundsitzungen die maximale Sitzungsdauer aus, indem Sie den Dropdown-Pfeil auswählen. Wählen Sie die Länge für die Sitzung aus und klicken Sie dann auf Speichern.

   > **Note**
   >
   > Änderungen der Sitzungsdauer gelten nur für neue Sitzungen. Aktuelle Sitzungen behalten ihre ursprüngliche Dauer bei.

7. Sie kehren zur Registerkarte Authentifizierung zurück. Über der Registerkarte wird eine grüne Benachrichtigung angezeigt, die darauf hinweist, dass die Sitzungseinstellungen erfolgreich aktualisiert wurden.

> **Note**
>
> Eine vom Kunden verwaltete Anwendung kann keine Benutzerhintergrundsitzung erstellen.

Erweiterte Sessions für Amazon Q Developer

Wenn Ihre Entwickler Amazon Q Developer als Teil einer integrierten Entwicklungsumgebung (IDE) verwenden, können Sie die Sitzungsdauer für Amazon Q Developer auf 90 Tage festlegen. Je nachdem, wann Sie IAM Identity Center aktiviert haben, ist die erweiterte Sitzungsdauer für Amazon Q Developer möglicherweise standardmäßig aktiviert. Diese erweiterte Sitzung hat keinen Einfluss auf die Sitzungsdauer des AWS Zugriffsportals oder anderer AWS verwalteter Anwendungen.

> **Note**
>
> Auf Amazon Q Developer kann von Konsolen aus zugegriffen werden, AWS-Regionen die auf kommerziell eingestellt sind und standardmäßig aktiviert sind. Wenn sich Ihre IAM Identity Center-Instance in einer Region befindet, in der Amazon Q Developer derzeit nicht zugänglich ist, wird die Standardeinstellung durch die Aktivierung der verlängerten Sitzungsdauer von 90 Tagen nicht außer Kraft gesetzt. Das bedeutet, dass Ihre Sitzungsdauer unverändert bleibt, unabhängig davon, ob Sie die erweiterte Sitzungsdauer von 90 Tagen aktivieren oder nicht. Weitere Informationen finden Sie unter Unterstützte AWS Regionen für Amazon Q Developer.

Um eine Sitzung für Amazon Q Developer zu verlängern

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Authentifizierung.
4. Wählen Sie unter Authentifizierung neben Sitzungsdauer die Option Konfigurieren aus. Das Dialogfeld Sitzungsdauer konfigurieren wird angezeigt.
5. Aktivieren Sie im Dialogfeld Sitzungsdauer konfigurieren das Kontrollkästchen Erweiterte Sitzungen für Amazon Q Developer aktivieren. Deaktivieren Sie das Kontrollkästchen, um erweiterte Sitzungssitzungen für Amazon Q Developer zu deaktivieren.
6. Wählen Sie Speichern, um zur Seite mit den Einstellungen zurückzukehren.

Aktive Sitzungen für Ihre Workforce-Benutzer anzeigen und beenden

Als IAM Identity Center-Administrator können Sie die Liste der aktiven Sitzungen Ihrer Workforce-Benutzer einsehen und bei Bedarf eine oder mehrere Sitzungen für einen Benutzer beenden. Beispielsweise müssen Sie möglicherweise die Sitzungen eines Benutzers beenden, wenn:

- Der Benutzer benötigt die Sitzungen nicht mehr.
- Der Benutzer sollte seinen aktuellen Authentifizierungsstatus nicht beibehalten. Dies kann der Fall sein, wenn sie das Unternehmen verlassen oder sich ihre Berechtigungen ändern.

Sie können diese Sitzungen mithilfe der IAM Identity Center-Konsole anzeigen und beenden. Ihre Benutzer können ihre eigenen Sitzungen auch über das AWS Zugriffsportal anzeigen und beenden.

Informationen darüber, wie Ihre Workforce-Benutzer ihre Sitzungen ohne Unterstützung eines Administrators aufrufen und beenden können, finden Sie unterIhre aktive Sitzung anzeigen und beenden.

> **Note**
>
> Durch das Beenden einer aktiven Sitzung für einen IAM Identity Center-Benutzer werden keine aktiven IAM-Rollensitzungen im AWS-Managementkonsole oder beendet. AWS CLI Weitere Informationen finden Sie unter Grundlegendes zu Authentifizierungssitzungen in IAM Identity Center.

Um eine aktive Sitzung für einen Workforce-Benutzer zu beenden (IAM Identity Center-Konsole)

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 aktiven Sitzungen für diesen Benutzer an.
5. Suchen Sie nach Benutzersitzungen im Hintergrund (optional)

   Um anhand des Amazon-Ressourcennamens (ARN) des Jobs, der die Sitzung verwendet, nach Sitzungen zu suchen, wählen Sie in der Liste Sitzungstyp die Option User background sessions aus und geben Sie dann den Job-ARN in das Suchfeld ein.

   > **Note**
   >
   > Sie können nur aktive Sitzungen beenden, die geladen sind. Wenn ein Benutzer viele Sitzungen hat, wählen Sie Weitere aktive Sitzungen laden, um weitere Sitzungen anzuzeigen.

6. Aktivieren Sie das Kontrollkästchen neben jeder Sitzung, die Sie beenden möchten, und wählen Sie dann Sitzungen beenden aus.
7. Es wird ein Dialogfeld angezeigt, das bestätigt, dass Sie die aktiven Sitzungen für diesen Benutzer beenden. Überprüfen Sie die Informationen, und wenn Sie fortfahren möchten, geben Sie den Text ein`confirm`, und wählen Sie dann Sitzungen beenden aus.

8. Sie kehren zur Seite des Benutzers zurück. Eine grüne Benachrichtigung zeigt an, dass die ausgewählten Sitzungen erfolgreich beendet wurden.

Überlegungen zur Sitzungsdauer bei der Verwendung von External IdPs, der AWS CLI und AWS SDKs

Im Folgenden finden Sie Überlegungen zur Konfiguration der Sitzungsdauer, wenn Sie einen externen Identitätsanbieter (IdP) oder die AWS Command Line Interface AWS Software Development Kits (SDKs) oder andere AWS Entwicklungstools für den programmgesteuerten Zugriff auf AWS Dienste verwenden.

Externe Identitätsanbieter, interaktive Benutzersitzungen und erweiterte Sitzungen für Amazon Q Developer

Wenn Sie einen externen Identitätsanbieter (IdP) verwenden und die Sitzungsdauer für benutzerinteraktive Sitzungen oder erweiterte Sitzungen für Amazon Q Developer konfigurieren, sollten Sie die folgenden Überlegungen berücksichtigen.

> **Note**
>
> Diese Überlegungen gelten nicht für Hintergrundsitzungen von Benutzern.

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.

AWS CLI und SDK-Sitzungen

Wenn Sie die AWS CLI oder andere AWS Entwicklungstools verwenden AWS SDKs, um programmgesteuert auf AWS Dienste zuzugreifen, müssen die folgenden Voraussetzungen erfüllt sein, um die Sitzungsdauer für das AWS Zugriffsportal und die AWS verwalteten Anwendungen festzulegen.

- 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

> **Note**
>
> Für Anwendungsfälle beim Kontozugriff gilt: Wenn Ihre Benutzer das ausführen AWS CLI, wenn Sie Ihren Berechtigungssatz aktualisieren, kurz bevor die IAM Identity Center-Sitzung abläuft und die Sitzungsdauer auf 20 Stunden festgelegt ist, während die Dauer des Berechtigungssatzes auf 12 Stunden festgelegt ist, läuft die AWS CLI Sitzung maximal 20

Stunden plus 12 Stunden, also insgesamt 32 Stunden. Weitere Informationen zur IAM Identity Center CLI finden Sie unter AWS CLI Befehlsreferenz.

Mindestversionen davon unterstützen SDKs die IAM Identity Center-Sitzungsverwaltung

Im Folgenden finden Sie die Mindestversionen von SDKs , 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: 1.18.0 credentials/ v1.13.0, config/v
JS V2	2.1253.0
JS V3	v3.210.0
C++	1.9.372
.NET	v3.7.400.0

Deaktivieren Sie den Benutzerzugriff auf und Anwendungen in IAM Identity AWS-Konten 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. Durch die Deaktivierung des Benutzerzugriffs können sie sich nicht mehr im AWS Zugriffsportal anmelden und sie haben

keinen Zugriff mehr auf die ihnen zugewiesenen Anwendungen AWS-Konten . Verwenden Sie „Benutzerzugriff deaktivieren“, um den Zugriff vorübergehend zu entfernen, wenn Sie den Zugriff möglicherweise später wiederherstellen müssen.

Gehen Sie wie folgt vor, um den Benutzerzugriff auf Ihr 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 Grundlegendes zu Authentifizierungssitzungen in IAM Identity Center.

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.

Verweigern Sie den Benutzerzugriff mit Service Control-Richtlinien

Um den Zugriff auf autorisierte API-Aufrufe sofort zu verweigern, wenn der Zugriff eines IAM Identity Center-Benutzers deaktiviert oder der Benutzer gelöscht wurde, können Sie:

1. Fügen Sie die Inline-Richtlinie für die dem Benutzer zugewiesenen Berechtigungssätze hinzu oder aktualisieren Sie sie, indem Sie einen expliziten `Deny` Effekt für alle Aktionen auf allen Ressourcen hinzufügen.
2. Geben Sie den `identitystore:userid` Bedingungsschlüssel `aws:userid` oder an.

Alternativ können Sie eine Service Control-Richtlinie verwenden, um dem Benutzer den Zugriff auf alle Mitgliedskonten in Ihrer Organisation zu verweigern.

Example Beispiel für ein SCP, um den Zugriff zu verweigern

Diese Verweigerungsrichtlinie blockiert alle AWS Aktionen für einen bestimmten Benutzer, unabhängig von anderen Berechtigungen, die ihm möglicherweise an anderer Stelle erteilt wurden. Diese Richtlinie hat Vorrang vor allen `Allow` Richtlinien.

JSON

```
{
    "Version":"2012-10-17",
    "Statement" : [
        {
            "Effect": "Deny",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                 "StringLike": {
                    "aws:UserId": "*:deleteduser@domain.com"
                }
            }
        }
    ]
}
```

JSON

```
{
    "Version":"2012-10-17",
    "Statement" : [
        {
            "Effect": "Deny",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                 "StringEquals": {
                    "identitystore:UserId": "DELETEDUSER_ID"
                }
            }
        }
    ]
}
```

Verwaltung des Zugriffs für Benutzer im Identity Center-Verzeichnis

Erfahren Sie, wie Sie Passwörter und Multi-Faktor-Authentifizierung (MFA) für Benutzer im IAM Identity Center-Verzeichnis verwalten. Diese Sicherheitsfunktionen tragen zum Schutz von Benutzerkonten bei.

> **Note**
>
> Diese Funktionen gelten nicht für Active Directory-Benutzer oder Benutzer eines externen Identitätsanbieters.

Administratoren können sowohl Passwörter als auch MFA über die IAM Identity Center-Konsole verwalten. Diese Sicherheitsfunktionen funktionieren nur mit dem integrierten Identity Center-Verzeichnis.

Verwaltung von Passwörtern

Die Passwortverwaltung umfasst die folgenden Funktionen:

- Passwörter mit E-Mail-Anweisungen zurücksetzen

- Generieren Sie Einmalpasswörter
- Konfigurieren Sie die automatische E-Mail-Überprüfung für per API erstellte Benutzer

AWS setzt feste Sicherheitsanforderungen durch, einschließlich Komplexitätsregeln und Beschränkungen für die Wiederverwendung von Passwörtern.

MFA

MFA ist standardmäßig aktiviert und unterstützt bis zu acht Geräte pro Benutzer.

Zu den unterstützten Gerätetypen gehören:

- Authenticator-Apps
- Sicherheitsschlüssel
- Integrierte biometrische Authentifikatoren

Administratoren können MFA-Geräte für Benutzer registrieren und verwalten.

Themen

- Benutzerkennwörter einrichten
- MFA für Identity Center-Verzeichnisbenutzer

Benutzerkennwörter einrichten

Für Benutzer, die im Identity Center-Verzeichnis erstellt wurden, können Administratoren Kennwortrichtlinien verwalten, Benutzer ohne Anfangskennwörter verwalten und Passwörter bei Bedarf zurücksetzen. Diese Funktionen zur Passwortverwaltung gelten nur für Benutzer im integrierten Identity Center-Verzeichnis. Wenn Sie Active Directory oder einen externen Identitätsanbieter verwenden, müssen Sie Passwörter in diesen Systemen verwalten.

Optionen für die Passwortverwaltung

- Passwortanforderungen — Sicherheitsanforderungen, die Benutzer erfüllen müssen, wenn sie Passwörter einrichten oder ändern. Dazu gehören Komplexitätsregeln und Einschränkungen der Wiederverwendung.

- Einrichtung eines Einmalpassworts — Konfigurieren Sie die E-Mail-Bestätigung für Benutzer, die über API oder CLI erstellt wurden und keine Anfangskennwörter haben. Sie können auch temporäre Passwörter für den sofortigen Zugriff generieren.
- Passwort-Resets — Setzen Sie Passwörter für Benutzer zurück, die gesperrt sind oder neue Anmeldeinformationen benötigen. Sie können Anweisungen zum Zurücksetzen per E-Mail senden oder Einmalpasswörter generieren.

Themen

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.

Einmalpasswort per E-Mail an Benutzer senden, die mit API oder CLI erstellt wurden

Wenn Sie Benutzer mit der CreateUserAPI-Operation oder dem `create-user` CLI-Befehl erstellen, haben die Benutzer keine Passwörter. Sie können die Einstellungen in IAM Identity Center aktualisieren, um diesen Benutzern nach ihrem ersten Anmeldeversuch eine Bestätigungs-E-Mail zu senden, sofern Sie bei der Erstellung eine E-Mail-Adresse für den Benutzer angegeben haben. Nach Erhalt der Bestätigungs-E-Mail muss der Benutzer ein Passwort für die Anmeldung festlegen.

Wenn Sie diese Einstellung nicht aktivieren, müssen Sie ein Einmalkennwort generieren und es mit Benutzern teilen, die Sie mit dem CreateUser API- oder `create-user` CLI-Befehl erstellen.

Um eine E-Mail zur Bestätigung der E-Mail-Adresse an Benutzer zu senden, die mit dem CreateUser API- oder **`create-user`** CLI-Befehl erstellt wurden

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Authentifizierung aus.
4. Wählen Sie im Abschnitt Standardauthentifizierung die Option Konfigurieren aus.
5. Aktivieren Sie im Dialogfeld Standardauthentifizierung konfigurieren das Kontrollkästchen E-Mail-OTP senden. Wählen Sie dann Save (Speichern) aus. Der Status wird von Deaktiviert auf Aktiviert aktualisiert.

Setzen Sie das IAM Identity Center-Benutzerkennwort für einen Endbenutzer zurück

Dieses Verfahren richtet sich an Administratoren, die das Passwort für einen Benutzer im 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. Das Benutzerkennwort Ihres AWS Access-Portals 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.

MFA für Identity Center-Verzeichnisbenutzer

> **Important**
>
> MFA in IAM Identity Center wird derzeit nicht für externe Identitätsanbieter unterstützt.

IAM Identity Center ist vorkonfiguriert und die Multi-Faktor-Authentifizierung (MFA) ist standardmäßig aktiviert, sodass sich alle Benutzer zusätzlich zu ihrem Benutzernamen und Passwort mit MFA anmelden müssen. Dadurch wird sichergestellt, dass sich Benutzer mithilfe der folgenden zwei Faktoren beim AWS Access Portal anmelden müssen:

- 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.

Themen

- MFA im IAM Identity Center konfigurieren
- Registrieren Sie ein MFA-Gerät für Benutzer
- Umbenennen und Löschen von MFA-Geräten in IAM Identity Center

Verfügbare MFA-Typen für IAM Identity Center

Die Multi-Faktor-Authentifizierung (MFA) ist ein einfacher und effektiver Mechanismus zur Verbesserung der Sicherheit Ihrer Benutzer. 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, wie etwa ein Sicherheitsschlüssel) oder Inhärenzfaktoren (etwas, das Sie sind, wie etwa 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, auf einem registrieren lassen. AWS-Konto Sie können die MFA-Einstellungen auch so konfigurieren, dass MFA immer dann erforderlich ist, wenn versucht wird, sich von einem neuen Gerät oder Browser aus anzumelden, oder wenn sie sich von einer unbekannten IP-Adresse aus anmelden. Weitere Informationen zur Konfiguration der MFA-Einstellungen für Ihre Benutzer finden Sie unter Wählen Sie MFA-Typen für die Benutzerauthentifizierung undMFA-Gerätedurchsetzung konfigurieren.

FIDO2 Authentifikatoren

FIDO2ist ein Standard, der Kryptografie mit öffentlichen Schlüsseln beinhaltet CTAP2 WebAuthnund darauf basiert. FIDO-Anmeldeinformationen sind Phishing-resistent, da sie nur für die Website gelten, auf der die Anmeldeinformationen erstellt wurden, z. B. AWS

AWS unterstützt 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

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. Directory Service beinhaltet 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 damit arbeiten Directory Service, z. B. Amazon RDS for SQL Server.

Wenn Ihr MFA auf der IAM Identity Center-Konsole deaktiviert ist und Sie RADIUS MFA mit konfiguriert haben 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 im IAM Identity Center konfigurieren

Sie können Multi-Faktor-Authentifizierungsfunktionen (MFA) in IAM Identity Center konfigurieren, 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.

Im Folgenden finden Sie allgemeine MFA-Empfehlungen, die von Ihren IAM Identity Center-Einstellungen und Unternehmenspräferenzen abhängen.

- 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 haben 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.
- Das folgende YouTube Video bietet einen Überblick über MFA und IAM Identity Center:

IAM Identity Center: Standardwerte für die Multi-Faktor-Authentifizierung für neue Instanzen

Themen

Benutzer zur MFA auffordern

Mithilfe der folgenden Schritte können Sie festlegen, wie oft Workforce-Benutzer bei jedem Versuch, sich am Access Portal anzumelden, zur Multi-Faktor-Authentifizierung (MFA) aufgefordert werden. AWS Bevor Sie beginnen, empfehlen wir Ihnen, das zu verstehen. Verfügbare MFA-Typen für IAM Identity Center

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

Note

Wenn Sie einen externen IdP verwenden, ist der Bereich Multi-Faktor-Authentifizierung nicht verfügbar. Ihr externer IdP, nicht IAM Identity Center, verwaltet die MFA-Einstellungen.

So konfigurieren Sie MFA

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 Authentifizierung aus.
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:

   - Jedes Mal, wenn sie sich anmelden (immer aktiv)

     In diesem Modus (Standardeinstellung) verlangt IAM Identity Center, dass Benutzer mit einem registrierten MFA-Gerät bei jeder Anmeldung dazu aufgefordert werden. Dies ist die sicherste Einstellung und stellt sicher, dass Ihre Organisations- oder Compliance-Richtlinien durchgesetzt werden, indem vorgeschrieben wird, dass MFA bei jeder Anmeldung am AWS Access Portal verwendet wird. PCI DSS empfiehlt beispielsweise nachdrücklich, bei jeder Anmeldung MFA für den Zugriff auf Anwendungen zu verwenden, die risikoreiche Zahlungsvorgänge unterstützen.

   - Nur wenn sich ihr Anmeldekontext ändert (kontextsensitiv)

     In diesem Modus 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, ist jedoch weniger sicher als die Always-On-Option. Benutzer werden nur dann zur Eingabe von MFA aufgefordert, wenn sich ihr Anmeldekontext ändert.

   - Nie (deaktiviert)

In diesem Modus melden sich alle Benutzer nur mit ihrem Standardbenutzernamen und Passwort an. Die Auswahl dieser Option deaktiviert IAM Identity Center MFA und wird nicht empfohlen.

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.

> **Note**
>
> Wenn Sie RADIUS MFA bereits mit verwenden und es weiterhin als Standard-MFA-Typ verwenden möchten 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 Änderungen speichern aus.

Verwandte Themen

- Wählen Sie MFA-Typen für die Benutzerauthentifizierung
- MFA-Gerätedurchsetzung konfigurieren
- Erlauben Sie Benutzern, ihre eigenen MFA-Geräte zu registrieren

Wählen Sie MFA-Typen für die Benutzerauthentifizierung

Gehen Sie wie folgt vor, um die Gerätetypen auszuwählen, mit denen sich Ihre Benutzer authentifizieren können, wenn sie im Access Portal zur Multi-Faktor-Authentifizierung (MFA) aufgefordert werden. AWS

So konfigurieren Sie MFA-Typen für Ihre Benutzer

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 Authentifizierung aus.
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.

   - Sicherheitsschlüssel und integrierte Authentifikatoren
   - Authenticator-Apps

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.

Weitere Informationen zu MFA in IAM finden Sie unter AWS Multi-Faktor-Authentifizierung in IAM.

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 Einstellungen aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Authentifizierung aus.
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

IAM Identity Center-Administratoren können Benutzern ermöglichen, ihre eigenen MFA-Geräte selbst zu registrieren.

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 Einstellungen aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Authentifizierung aus.
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. Ihr Gerät für MFA registrieren Dieses Thema enthält Anweisungen zum Einrichten ihrer eigenen MFA-Geräte.

Registrieren Sie ein MFA-Gerät für Benutzer

IAM Identity Center-Administratoren können in der IAM Identity Center-Konsole ein neues MFA-Gerät für den Zugriff durch einen bestimmten Benutzer einrichten. Administratoren 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.

Umbenennen und Löschen von MFA-Geräten in IAM Identity Center

IAM Identity Center-Administratoren können die folgenden Verfahren verwenden, um das MFA-Gerät eines Benutzers umzubenennen oder zu löschen.

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.

Konfigurieren Sie den Zugriff auf Anwendungen

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 Anwendung 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-Managementkonsole für Ihre Organisation bestimmten AWS-Konto Daten gewähren. Weitere Informationen finden Sie unter Konfigurieren Sie den Zugriff auf AWS-Konten.

Themen

AWS verwaltete Anwendungen

AWS IAM Identity Center optimiert und vereinfacht die Aufgabe, die Benutzer Ihrer Belegschaft mit AWS verwalteten Anwendungen wie Amazon Q Developer und Amazon Quick Suite zu verbinden. Mit IAM Identity Center können Sie Ihren bestehenden Identitätsanbieter einmalig verbinden und Benutzer und Gruppen aus Ihrem Verzeichnis synchronisieren oder Ihre Benutzer direkt in IAM Identity Center erstellen und verwalten. Durch die Bereitstellung eines zentralen Verbundpunkts macht IAM Identity Center die Einrichtung eines Verbunds oder der Benutzer- und Gruppensynchronisierung für jede Anwendung überflüssig und reduziert Ihren Verwaltungsaufwand. Außerdem erhalten Sie eine gemeinsame Ansicht der Benutzer- und Gruppenzuweisungen.

Eine Tabelle der AWS Anwendungen, die mit IAM Identity Center funktionieren, finden Sie unterAWS verwaltete Anwendungen, die Sie mit IAM Identity Center verwenden können.

Steuern des Zugriffs auf AWS verwaltete Anwendungen

Der Zugriff auf AWS verwaltete Anwendungen wird auf zwei Arten gesteuert:

- Erster Zugriff auf die Anwendung

  Das IAM Identity Center verwaltet dies durch Zuweisungen an die Anwendung. Standardmäßig sind Zuweisungen für AWS verwaltete Anwendungen erforderlich. Wenn Sie ein Anwendungsadministrator sind, können Sie wählen, ob Zuweisungen zu einer Anwendung erforderlich sind.

  Wenn Zuweisungen erforderlich sind, können bei der Anmeldung von Benutzern nur Benutzer AWS-Zugangsportal, die der Anwendung direkt oder über eine Gruppenzuweisung zugewiesen wurden, die Anwendungskachel anzeigen.

  Wenn keine Zuweisungen erforderlich sind, können Sie allen IAM Identity Center-Benutzern den Zugriff auf die Anwendung ermöglichen. In diesem Fall verwaltet die Anwendung den Zugriff auf Ressourcen und die Anwendungskachel ist für alle Benutzer sichtbar, die die Anwendung besuchen. AWS-Zugangsportal

  > **Important**
  >
  > 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 Ihnen, sich mit

dem Anwendungsadministrator abzustimmen. 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.

- Zugriff auf Anwendungsressourcen

  Die Anwendung verwaltet dies durch unabhängige Ressourcenzuweisungen, die sie kontrolliert.

AWS Verwaltete Anwendungen bieten eine administrative Benutzeroberfläche, mit der Sie den Zugriff auf Anwendungsressourcen verwalten können. Beispielsweise können Quick Suite-Administratoren Benutzern basierend auf ihrer Gruppenmitgliedschaft den Zugriff auf Dashboards zuweisen. Die meisten AWS verwalteten Anwendungen bieten auch eine AWS-Managementkonsole 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.

Weitergabe von Identitätsinformationen

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.
- Alternativ können Sie mithilfe von Dienststeuerungsrichtlinien (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 damit allen Anwendungen SCPs den Zugriff verbieten, mit Ausnahme derjenigen, die Sie zulassen möchten.

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

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 Benutzer im Identity Center-Verzeichnis 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. Microsoft ADVerzeichnis
  - Externer Identitätsanbieter — Weitere Informationen finden Sie unterExterne Identitätsanbieter.

  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.

Einschränkung der Nutzung AWS verwalteter Anwendungen

Wenn Sie IAM Identity Center zum ersten Mal aktivieren, steht es als Identitätsquelle für AWS verwaltete Anwendungen für alle Konten in Ihrem Konto zur Verfügung. AWS Organizations Um

Anwendungen einzuschränken, müssen Sie Richtlinien zur Servicesteuerung implementieren ()SCPs. SCPs sind eine Funktion, mit der Sie AWS Organizations die maximalen Berechtigungen, die Identitäten (Benutzer und Rollen) in Ihrer Organisation haben können, zentral steuern können. Sie können SCPs sie 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. Weitere Informationen finden Sie unter Richtlinien zur Servicesteuerung (SCPs) im AWS Organizations Benutzerhandbuch.

Das folgende SCP-Beispiel blockiert den Zugriff auf die Benutzer- und Gruppeninformationen von IAM Identity Center und verhindert, dass die Anwendung gestartet wird, außer in bestimmten Konten (111111111111 und 222222222222):

```
{
  "Sid": "DenyIdCExceptInDesignatedAWSAccounts",
  "Effect": "Deny",
  "Action": [
    "identitystore:*",
    "sso:*",
    "sso-directory:*",
    "sso-oauth:*"
  ],
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "aws:PrincipalAccount": [
        "111111111111",
        "222222222222"
      ]
    }
  }
}
```

AWS verwaltete Anwendungen, die Sie mit IAM Identity Center verwenden können

Mit IAM Identity Center können Sie Ihre bestehende Identitätsquelle verbinden oder Benutzer einmalig erstellen. Auf diese Weise können Anwendungsadministratoren den Zugriff auf die folgenden AWS verwalteten Anwendungen ohne separaten Verbund oder Benutzer- und Gruppensynchronisierung verwalten.

Alle AWS verwalteten Anwendungen in der folgenden Tabelle lassen sich in Organisationsinstanzen von IAM Identity Center integrieren. Die Tabelle enthält auch Informationen zu den folgenden Informationen für eine unterstützte AWS verwaltete Anwendung:

- Ob die Anwendung auch in Kontoinstanzen von IAM Identity Center integriert werden kann
- Ob die Anwendung die Verbreitung vertrauenswürdiger Identitäten über IAM Identity Center ermöglichen kann
- Ob die Anwendung IAM Identity Center unterstützt, das mit einem vom Kunden verwalteten KMS-Schlüssel konfiguriert ist

AWS verwaltete Anwendungen, die in IAM Identity Center integriert sind

AWS verwaltete Anwendung	Integriert in Kontoinstanzen von IAM Identity Center	Ermöglicht die Verbreitung vertrauenswürdiger Identitäten über IAM Identity Center	Unterstützt IAM Identity Center, das mit einem vom Kunden verwalteten KMS-Schlüssel konfiguriert ist
WorkSpaces Amazon-Anwendungen	Nein	Nein	Nein
Amazon Athena SQL	Ja	Ja	Ja
Amazon CodeCatalyst	Ja	Nein	Nein
Amazon Connect	Nein	Nein	Nein
Amazon DataZone	Ja	Ja	Ja
Amazon EMR bei Amazon EC2	Ja	Ja	Ja

AWS verwaltete Anwendung	Integriert in Kontoinstanzen von IAM Identity Center	Ermöglicht die Verbreitung vertrauenswürdiger Identitäten über IAM Identity Center	Unterstützt IAM Identity Center, das mit einem vom Kunden verwalteten KMS-Schlüssel konfiguriert ist
Amazon EMR Serverless	Ja	Ja	Nein
Amazon EMR Studio	Ja	Ja	Ja
Amazon Kendra	Nein	Nein	Ja
Amazon Managed Grafana	Nein	Nein	Nein
Amazon Monitron	Nein	Nein	Nein
OpenSearch Amazon-Dienst	Ja	Ja	Nein
OpenSearch Amazon-Dienst Serverless Service	Ja	Ja	Ja
OpenSearch user interface (Dashboards)	Ja	Ja	Ja
Amazon Q Business	Ja	Ja	Ja
Amazon Q Developer	Ja*	Ja	Nein

AWS verwaltete Anwendung	Integriert in Kontoinstanzen von IAM Identity Center	Ermöglicht die Verbreitung vertrauenswürdiger Identitäten über IAM Identity Center	Unterstützt IAM Identity Center, das mit einem vom Kunden verwalteten KMS-Schlüssel konfiguriert ist
Amazon Quick Suite	Ja	Ja	Ja
Amazon Redshift	Ja	Ja	Nein
Amazon S3 Access Grants	Ja	Ja	Ja
SageMaker Vereinheitlichtes Amazon Studio	Ja	Ja	Ja
Amazon SageMaker Studio	Nein	Ja	Nein
Amazon WorkMail	Ja	Ja	Ja
Amazon WorkSpaces	Ja	Nein	Nein
Amazon WorkSpaces Secure Browser	Nein	Nein	Ja
AWS App Studio	Ja	Nein	Nein
AWS Client VPN	Nein	Nein	Nein

AWS verwaltete Anwendung	Integriert in Kontoinstanzen von IAM Identity Center	Ermöglicht die Verbreitung vertrauenswürdiger Identitäten über IAM Identity Center	Unterstützt IAM Identity Center, das mit einem vom Kunden verwalteten KMS-Schlüssel konfiguriert ist
AWS CLI	Nein	Nein	Nein
AWS Deadline Cloud	Ja	Nein	Nein
AWS Glue	Ja	Ja	Nein
AWS IoT Events	Nein	Nein	Nein
AWS IoT Fleet Hub	Nein	Nein	Nein
AWS IoT SiteWise	Nein	Nein	Nein
AWS Lake Formation	Ja	Ja	Nein
AWS re:Post Private	Ja	Nein	Nein
AWS Supply Chain	Ja	Nein	Nein
AWS Systems Manager	Nein	Nein	Ja

AWS verwaltete Anwendung	Integriert in Kontoinstanzen von IAM Identity Center	Ermöglicht die Verbreitung vertrauenswürdiger Identitäten über IAM Identity Center	Unterstützt IAM Identity Center, das mit einem vom Kunden verwalteten KMS-Schlüssel konfiguriert ist
AWS Transfer Family Web-Apps	Ja	Ja	Nein
AWS Transformation	Ja	Nein	Ja
AWS Verified Access	Nein	Nein	Ja
Mehrparteien-Genehmigung	Nein	Ja	Ja

* Für Amazon Q Developer werden Kontoinstanzen von IAM Identity Center unterstützt, es sei denn, Ihre Benutzer benötigen Zugriff auf alle Amazon Q Developer-Funktionen auf AWS Websites. Weitere Informationen finden Sie unter Einrichtung von Amazon Q Developer im Amazon Q Developer User Guide.

Schnellstart: Einrichtung von IAM Identity Center zum Testen AWS verwalteter Anwendungen

Wenn Ihr Administrator Ihnen noch keinen Zugriff auf IAM Identity Center gewährt hat, können Sie die Schritte in diesem Thema verwenden, um IAM Identity Center zum Testen AWS verwalteter Anwendungen einzurichten. Sie erfahren, wie Sie IAM Identity Center aktivieren, einen Benutzer direkt in IAM Identity Center erstellen und diesen Benutzer einer verwalteten Anwendung zuweisen. AWS

Dieses Thema enthält Schnellstartschritte zur Aktivierung von IAM Identity Center auf eine der folgenden Arten:

- Mit AWS Organizations — Wenn Sie diese Option wählen, wird eine Organisationsinstanz von IAM Identity Center erstellt.
- Nur in Ihrem speziellen Fall AWS-Konto— Wenn Sie diese Option wählen, wird eine Kontoinstanz von IAM Identity Center erstellt.

Informationen zu diesen Instance-Typen finden Sie unterOrganisations- und Kontoinstanzen von IAM Identity Center.

Voraussetzungen

Bevor Sie IAM Identity Center aktivieren, überprüfen Sie Folgendes:

- Sie haben eine AWS-Konto — Falls Sie noch keine haben AWS-Konto, finden Sie weitere Informationen unter Erste Schritte mit einer AWS-Konto im Referenzhandbuch zur AWS Kontoverwaltung.
- Die AWS verwaltete Anwendung funktioniert mit IAM Identity Center — Überprüfen Sie anhand der AWS verwaltete Anwendungen, die Sie mit IAM Identity Center verwenden können Liste, ob die AWS verwaltete Anwendung, die Sie testen möchten, mit IAM Identity Center funktioniert.
- Sie haben die regionalen Überlegungen gelesen. Stellen Sie sicher, dass die AWS verwaltete Anwendung, die Sie testen möchten, in dem Land unterstützt wird, in AWS-Region dem Sie IAM Identity Center aktivieren. Weitere Informationen finden Sie in der Dokumentation zur AWS verwalteten Anwendung.

> **Note**
>
> Sie müssen Ihre AWS verwaltete Anwendung in derselben Region bereitstellen, in der Sie IAM Identity Center aktivieren möchten.

Einrichtung einer Organisationsinstanz von IAM Identity Center zum Testen AWS verwalteter Anwendungen

> **Note**
>
> In diesem Thema wird beschrieben, wie IAM Identity Center aktiviert wird. Dies ist die empfohlene Methode zur Aktivierung von IAM Identity Center. AWS Organizations

Bestätigen Sie Ihre Berechtigungen

Um IAM Identity Center mit zu aktivieren AWS Organizations, müssen Sie sich mit einer der folgenden Methoden bei der AWS Management Console anmelden:

- Ein Benutzer mit Administratorrechten in dem Bereich, in AWS-Konto dem IAM Identity Center aktiviert wird. AWS Organizations
- Der Root-Benutzer (nicht empfohlen, es sei denn, es gibt keine anderen Administratorbenutzer).

> **Important**
>
> Der Root-Benutzer hat Zugriff auf alle AWS Dienste und Ressourcen im Konto. Aus Sicherheitsgründen sollten Sie nicht die Root-Anmeldeinformationen Ihres Kontos für den Zugriff auf AWS Ressourcen verwenden, es sei denn, Sie haben keine anderen Anmeldeinformationen. Diese Anmeldeinformationen bieten uneingeschränkten Zugriff auf Konten und können nur schwer widerrufen werden.

Schritt 1. Aktivieren Sie IAM Identity Center mit AWS Organizations

1. Gehen Sie wie folgt vor, um sich bei der AWS-Managementkonsole 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 AWS bereits eine eigenständige Version AWS-Konto (IAM-Anmeldeinformationen) — Melden Sie sich mit Ihren IAM-Anmeldeinformationen und Administratorrechten an.
2. Wählen Sie auf der Startseite der AWS Management Console den IAM Identity Center-Dienst aus oder navigieren Sie zur IAM Identity Center-Konsole.
3. Wählen Sie Aktivieren und aktivieren Sie IAM Identity Center mit. AWS Organizations Wenn Sie dies tun, erstellen Sie eine Organisationsinstanz von IAM Identity Center.

Schritt 2. Erstellen Sie einen Administratorbenutzer in IAM Identity Center

Dieses Verfahren beschreibt, wie Sie einen Benutzer direkt im integrierten Identity Center-Verzeichnis erstellen. Dieses Verzeichnis ist mit keinem anderen Verzeichnis verbunden, das Ihr Administrator möglicherweise zur Verwaltung von Workforce-Benutzern verwendet. Nachdem Sie den Benutzer in

IAM Identity Center erstellt haben, geben Sie neue Anmeldeinformationen für diesen Benutzer an. Wenn Sie sich als dieser Benutzer anmelden, um Ihre AWS verwaltete Anwendung zu testen, melden Sie sich mit den neuen Anmeldeinformationen an, nicht mit den vorhandenen Anmeldeinformationen, die Sie für den Zugriff auf Unternehmensressourcen verwenden.

> **Note**
>
> Wir empfehlen, dass Sie diese Methode nur zu Testzwecken verwenden, um Benutzer zu erstellen.

1. Wählen Sie im Navigationsbereich der IAM Identity Center-Konsole Benutzer und dann Benutzer hinzufügen aus.
2. Folgen Sie den Anweisungen in der Konsole, um den Benutzer hinzuzufügen. Wählen Sie „E-Mail an diesen Benutzer mit Anweisungen zur Passworteinrichtung senden“ aus und stellen Sie sicher, dass Sie eine E-Mail-Adresse angeben, auf die Sie Zugriff haben.
3. Wählen Sie AWS-Konten im Navigationsbereich das Kontrollkästchen neben Ihrem Konto aus und wählen Sie Benutzer oder Gruppen zuweisen aus.
4. Wählen Sie die Registerkarte Benutzer, aktivieren Sie das Kontrollkästchen neben dem Benutzer, den Sie gerade hinzugefügt haben, und klicken Sie auf Weiter.
5. Wählen Sie „Berechtigungssatz erstellen“ und folgen Sie den Anweisungen in der Konsole, um den `AdministratorAccess` vordefinierten Berechtigungssatz zu erstellen.
6. Wenn Sie fertig sind, wird der neue Berechtigungssatz in der Liste angezeigt. Schließen Sie die Registerkarte Berechtigungssätze in Ihrem Browserfenster, kehren Sie zur Registerkarte Benutzer und Gruppen zuweisen zurück und wählen Sie das Aktualisierungssymbol neben Berechtigungssatz erstellen.
7. Auf der Browser-Registerkarte „Benutzer und Gruppen zuweisen“ wird der neue Berechtigungssatz in der Liste angezeigt. Aktivieren Sie das Kontrollkästchen neben dem Namen des Berechtigungssatzes, klicken Sie auf Weiter und dann auf Absenden.
8. Melden Sie sich bei der -Konsole ab.

Schritt 3. Melden Sie sich als Administratorbenutzer beim AWS Access Portal an

Das AWS Zugriffsportal ist ein Webportal, das dem von Ihnen erstellten Benutzer Zugriff auf die AWS Managementkonsole bietet. Bevor Sie sich beim AWS Access Portal anmelden können, müssen

Sie die Einladung zum Beitritt zu IAM Identity Center annehmen und Ihre Benutzeranmeldedaten aktivieren.

1. Suchen Sie in Ihrer E-Mail nach der Betreffzeile Einladung zum Beitritt zu AWS IAM Identity Center.
2. Wählen Sie Einladung annehmen und folgen Sie den Anweisungen auf der Anmeldeseite, um ein neues Passwort festzulegen, sich anzumelden und ein MFA-Gerät für Ihren Benutzer zu registrieren.
3. Nachdem Sie Ihr MFA-Gerät registriert haben, wird das AWS Zugriffsportal geöffnet.
4. Wählen Sie im AWS Zugriffsportal Ihre aus AWS-Konto und wählen Sie AdministratorAccess. Sie werden zur AWS Management Console weitergeleitet.

Schritt 4. Konfigurieren Sie die AWS verwaltete Anwendung für die Verwendung von IAM Identity Center

1. Während Sie bei der AWS Management Console angemeldet sind, öffnen Sie die Konsole für die AWS verwaltete Anwendung, die Sie verwenden möchten.
2. Folgen Sie den Anweisungen in der Konsole, um die AWS verwaltete Anwendung für die Verwendung von IAM Identity Center zu konfigurieren. Während dieses Vorgangs können Sie den Benutzer, den Sie erstellt haben, der Anwendung zuweisen.

Einrichtung einer Kontoinstanz von IAM Identity Center zum Testen AWS verwalteter Anwendungen

> **Note**
>
> Eine Kontoinstanz von IAM Identity Center beschränkt Ihre Bereitstellung auf eine einzige AWS-Konto. Sie müssen diese Instanz in derselben Weise aktivieren AWS-Region wie die AWS Anwendung, die Sie testen möchten.

Bestätigen Sie Ihre App

Alle AWS verwalteten Anwendungen, die mit IAM Identity Center funktionieren, können mit Organisationsinstanzen von IAM Identity Center verwendet werden. Allerdings können nur einige

dieser Anwendungen mit Kontoinstanzen von IAM Identity Center verwendet werden. Sehen Sie sich die Liste von an. AWS verwaltete Anwendungen, die Sie mit IAM Identity Center verwenden können

Schritt 1. Aktivieren Sie eine Kontoinstanz von IAM Identity Center

1. Gehen Sie wie folgt vor, um sich bei der AWS-Managementkonsole 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 AWS bereits eine eigenständige Version AWS-Konto (IAM-Anmeldeinformationen) — Melden Sie sich mit Ihren IAM-Anmeldeinformationen und Administratorrechten an.
2. Wählen Sie auf der Startseite der AWS Management Console den IAM Identity Center-Dienst aus oder navigieren Sie zur IAM Identity Center-Konsole.
3. Wählen Sie Enable (Aktivieren) aus.
4. Wählen Sie auf der AWS Organizations Seite „IAM Identity Center aktivieren mit“ die Option Eine Kontoinstanz von IAM Identity Center aktivieren aus.
5. Überprüfen Sie auf der Seite Kontoinstanz von IAM Identity Center aktivieren die Informationen und fügen Sie optional Tags hinzu, die Sie dieser Kontoinstanz zuordnen möchten. Wählen Sie dann Aktivieren.

Schritt 2. Erstellen Sie einen Benutzer im IAM Identity Center

Dieses Verfahren beschreibt, wie Sie einen Benutzer direkt im integrierten Identity Center-Verzeichnis erstellen. Dieses Verzeichnis ist mit keinem anderen Verzeichnis verbunden, das Ihr Administrator möglicherweise zur Verwaltung von Workforce-Benutzern verwendet. Nachdem Sie den Benutzer in IAM Identity Center erstellt haben, geben Sie neue Anmeldeinformationen für diesen Benutzer an. Wenn Sie sich als dieser Benutzer anmelden, um Ihre AWS verwaltete Anwendung zu testen, melden Sie sich mit den neuen Anmeldeinformationen an. Mit den neuen Anmeldeinformationen können Sie nicht auf andere Unternehmensressourcen zugreifen.

> **Note**
>
> Es wird empfohlen, diese Methode nur zu Testzwecken zum Erstellen von Benutzern zu verwenden.

1. Wählen Sie im Navigationsbereich der IAM Identity Center-Konsole Benutzer und dann Benutzer hinzufügen aus.
2. Folgen Sie den Anweisungen in der Konsole, um den Benutzer hinzuzufügen. Wählen Sie „E-Mail an diesen Benutzer mit Anweisungen zur Passworteinrichtung senden“ aus und stellen Sie sicher, dass Sie eine E-Mail-Adresse angeben, auf die Sie Zugriff haben.
3. Melden Sie sich bei der -Konsole ab.

Schritt 3. Melden Sie sich als Ihr IAM Identity Center-Benutzer beim AWS Zugriffsportal an

Das AWS Zugriffsportal ist ein Webportal, das dem von Ihnen erstellten Benutzer Zugriff auf die AWS Managementkonsole bietet. Bevor Sie sich beim AWS Access Portal anmelden können, müssen Sie die Einladung zum Beitritt zu IAM Identity Center annehmen und Ihre Benutzeranmeldedaten aktivieren.

1. Suchen Sie in Ihrer E-Mail nach der Betreffzeile Einladung zum Beitritt zu AWS IAM Identity Center.
2. Wählen Sie Einladung annehmen und folgen Sie den Anweisungen auf der Anmeldeseite, um ein neues Passwort festzulegen, sich anzumelden und ein MFA-Gerät für Ihren Benutzer zu registrieren.
3. Nachdem Sie Ihr MFA-Gerät registriert haben, wird das AWS Zugriffsportal geöffnet. Wenn Ihnen Anwendungen zur Verfügung stehen, finden Sie sie auf der Registerkarte Anwendungen.

> **Note**
>
> AWS Anwendungen, die Kontoinstanzen unterstützen, ermöglichen es Benutzern, sich bei Anwendungen anzumelden, ohne dass zusätzliche Berechtigungen erforderlich sind. Daher bleibt die Registerkarte Konten leer.

Schritt 4. Konfigurieren Sie die AWS verwaltete Anwendung für die Verwendung von IAM Identity Center

1. Während Sie bei der AWS Management Console angemeldet sind, öffnen Sie die Konsole für die AWS verwaltete Anwendung, die Sie verwenden möchten.
2. Folgen Sie den Anweisungen in der Konsole, um die AWS verwaltete Anwendung für die Verwendung von IAM Identity Center zu konfigurieren. Während dieses Vorgangs können Sie den Benutzer, den Sie erstellt haben, der Anwendung zuweisen.

Details zu einer AWS verwalteten Anwendung anzeigen und ändern

Nachdem Sie eine AWS verwaltete Anwendung über die Konsole oder 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 Details zur Anwendung in der IAM Identity Center-Konsole anzeigen und ändern.

Zu den Informationen über die Anwendung gehören, ob Benutzer- und Gruppenzuweisungen erforderlich sind, und gegebenenfalls die zugewiesenen Benutzer und Gruppen sowie vertrauenswürdige Anwendungen für die Weitergabe von Identitäten. Hinweise zur Weitergabe vertrauenswürdiger Identitäten finden Sie unterÜberblick über die Verbreitung vertrauenswürdiger Identitäten.

So können Sie Informationen zu einer AWS verwalteten Anwendung in der IAM Identity Center-Konsole anzeigen und ändern

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie Applications (Anwendungen).
3. Wählen Sie die Registerkarte „AWS Verwaltet“.
4. Wählen Sie den Link für die verwaltete Anwendung, die Sie öffnen und ansehen möchten.
5. Wenn Sie Informationen zu einer AWS verwalteten Anwendung ändern möchten, wählen Sie Aktion und dann Details bearbeiten.
6. Sie können den Anzeigenamen und die Beschreibung der Anwendung sowie die Zuweisungsmethode für Benutzer und Gruppen ändern.

    a. Um den Anzeigenamen zu ändern, geben Sie den gewünschten Namen in das Feld Anzeigename ein und wählen Sie Änderungen speichern.

    b. Um die Beschreibung zu ändern, geben Sie die gewünschte Beschreibung in das Feld Beschreibung ein und wählen Sie Änderungen speichern.

    c. Um die Zuweisungsmethode für Benutzer und Gruppen zu ändern, nehmen Sie die gewünschte Änderung vor und wählen Sie Änderungen speichern. Weitere Informationen finden Sie unter the section called “Benutzer, Gruppen und Bereitstellung”.

Deaktivierung einer AWS verwalteten Anwendung

Um zu verhindern, dass sich Benutzer bei einer AWS verwalteten Anwendung authentifizieren, können Sie die Anwendung in der IAM Identity Center-Konsole deaktivieren.

Um eine verwaltete Anwendung zu AWS 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 deaktivieren“ die Option „Deaktivieren“.
6. In der Liste der AWS verwalteten Anwendungen wird der Anwendungsstatus als Inaktiv angezeigt.

> **Note**
>
> Wenn eine AWS verwaltete Anwendung deaktiviert ist, können Sie die Fähigkeit der Benutzer wiederherstellen, sich bei der Anwendung zu authentifizieren, indem Sie Aktionen und dann Aktivieren wählen.

Konsolensitzungen mit verbesserter Identität aktivieren

Eine Sitzung mit verbesserter Identität für die Konsole verbessert die Konsolensitzung eines Benutzers AWS , indem sie zusätzlichen Benutzerkontext bereitstellt, um die Benutzererfahrung zu personalisieren. Diese Funktion wird derzeit für Amazon Q Developer Pro-Benutzer von Amazon Q in AWS Apps und Websites unterstützt.

Sie können Konsolensitzungen mit verbesserter Identität aktivieren, ohne Änderungen an den bestehenden Zugriffsmustern oder dem Verbund mit der AWS Konsole vorzunehmen. 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 Konsolensitzungen mit erweiterter Identität aktivieren, sollten Sie sich mit den folgenden Voraussetzungen und Überlegungen vertraut machen:

- Wenn Ihre Benutzer über ein Amazon Q Developer Pro-Abonnement über AWS Apps und Websites auf Amazon Q zugreifen, müssen Sie identitätserweiterte Konsolensitzungen aktivieren.

  > **Note**
  >
  > Amazon Q Developer-Benutzer können ohne identitätserweiterte Sitzungen auf Amazon Q zugreifen, haben jedoch keinen Zugriff auf ihre Amazon Q Developer Pro-Abonnements.

- Konsolensitzungen mit erweiterter Identität 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.
- Um Konsolensitzungen mit verbesserter Identität zu aktivieren, benötigen Sie die folgenden Berechtigungen:
  - `sso:CreateApplication`
  - `sso:GetSharedSsoConfiguration`
  - `sso:ListApplications`
  - `sso:PutApplicationAssignmentConfiguration`
  - `sso:PutApplicationAuthenticationMethod`
  - `sso:PutApplicationGrant`
  - `sso:PutApplicationAccessScope`
  - `signin:CreateTrustedIdentityPropagationApplicationForConsole`
  - `signin:ListTrustedIdentityPropagationApplicationsForConsole`

- Damit Ihre Benutzer Konsolensitzungen mit verbesserter Identität verwenden können, müssen Sie ihnen die entsprechenden `sts:setContext` Berechtigungen in einer identitätsbasierten Richtlinie erteilen. Weitere Informationen finden Sie unter Benutzern Berechtigungen zur Nutzung von Konsolensitzungen mit erweiterter Identität gewähren.

Wie aktiviert man Sitzungen identity-enhanced-console

Sie können Konsolensitzungen mit verbesserter Identität in der Amazon Q-Konsole oder in der IAM Identity Center-Konsole aktivieren.

Konsolensitzungen mit verbesserter Identität in der Amazon Q-Konsole aktivieren

Bevor Sie Konsolensitzungen mit erweiterter Identität 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 IAM Identity Center aktivieren.
2. Connect Ihre Identitätsquelle mit IAM Identity Center und stellen Sie Benutzern Zugriff auf IAM Identity Center zur Verfügung. Sie können Ihre bestehende Identitätsquelle mit IAM Identity Center verbinden oder das Identity Center-Verzeichnis verwenden, falls Sie nicht bereits eine andere Identitätsquelle verwenden. Weitere Informationen finden Sie unter Tutorials zu Identitätsquellen im IAM Identity Center.
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 Konsolensitzungen mit verbesserter Identität aktivieren.

> **Note**
>
> Wenn Sie nicht über ausreichende Berechtigungen verfügen, um Konsolensitzungen mit erweiterter Identität 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 Konsolensitzungen mit erweiterter Identität in der IAM Identity Center-Konsole

Wenn Sie ein IAM Identity Center-Administrator sind, werden Sie möglicherweise von einem anderen Administrator aufgefordert, identitätserweiterte 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 „Sitzungen mit erweiterter Identität aktivieren“ die Option Aktivieren aus.
4. Wählen Sie in der zweiten Nachricht die Option Aktivieren aus.
5. Nachdem Sie die Aktivierung von Konsolensitzungen mit verbesserter Identität abgeschlossen haben, wird oben auf der Einstellungsseite eine Bestätigungsmeldung angezeigt.
6. Im Abschnitt Details lautet der Status für Identity-Enhanced Sessions auf Aktiviert.

So funktionieren Konsolensitzungen mit verbesserter Identität

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 mit erweiterter Identität 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.

Vom Kunden verwaltete Anwendungen

IAM Identity Center fungiert als zentraler Identitätsdienst für die Benutzer und Gruppen Ihrer Belegschaft. 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. Mit einer einzigen Verbindung stellt IAM Identity Center Ihren IdP vor mehreren dar AWS-Services und ermöglicht es Ihren OAuth 2.0-Anwendungen, im Namen Ihrer Benutzer Zugriff auf Daten in diesen Diensten anzufordern. Sie können IAM Identity Center auch verwenden, um Ihren Benutzern Zugriff auf SAML 2.0-Anwendungen zuzuweisen.

- Wenn Ihre Anwendung JSON Web Tokens (JWTs) unterstützt, können Sie die Funktion zur Verbreitung vertrauenswürdiger Identitäten von IAM Identity Center verwenden, damit Ihre Anwendung im Namen Ihrer Benutzer Zugriff AWS-Services auf Daten anfordern kann. Trusted Identity Propagation basiert auf dem OAuth 2.0 Authorization Framework und beinhaltet eine Option für Anwendungen, Identitätstoken, die von einem externen OAuth 2.0-Autorisierungsserver stammen, gegen Token auszutauschen, die von IAM Identity Center ausgestellt und von IAM Identity Center anerkannt wurden. AWS-Services Weitere Informationen finden Sie unter Anwendungsfälle zur Verbreitung vertrauenswürdiger Identitäten.
- Wenn Ihre Anwendung SAML 2.0 unterstützt, können Sie sie mit einer Organisationsinstanz von IAM Identity Center verbinden. Sie können IAM Identity Center verwenden, um Ihrer SAML 2.0-Anwendung Zugriff zuzuweisen.

Themen

- Single Sign-On-Zugriff auf SAML 2.0- und 2.0-Anwendungen OAuth
- Einrichtung von vom Kunden verwalteten SAML 2.0-Anwendungen

Single Sign-On-Zugriff auf SAML 2.0- und 2.0-Anwendungen OAuth

Mit IAM Identity Center können Sie Ihren Benutzern Single Sign-On-Zugriff auf SAML 2.0- oder 2.0-Anwendungen gewähren. OAuth Die folgenden Themen bieten einen allgemeinen Überblick über SAML 2.0 und 2.0. OAuth

Themen

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

> **Note**
>
> IAM Identity Center unterstützt nicht die Überprüfung von Signaturen eingehender SAML-Authentifizierungsanfragen von SAML-Anwendungen.

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 Zugang 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 2.0 für die Authentifizierung verwendet wird. OAuth Über den IAM Identity Center OIDC-Dienst registriert eine Anwendung einen OAuth 2.0-Client und verwendet einen dieser Datenflüsse APIs, um ein Zugriffstoken abzurufen, das Berechtigungen für IAM Identity Center protected gewährt. APIs Eine Anwendung gibt Zugriffsbereiche an, 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 2.0-Grant-Flow OAuth verwendet

OAuth 2.0-Zuschussflüsse sind nur über AWS verwaltete Anwendungen verfügbar, die die Zuschüsse unterstützen. Um einen OAuth 2.0-Flow zu verwenden, müssen Ihre Instanz von IAM Identity Center und alle unterstützten AWS verwalteten Anwendungen, die Sie verwenden, in einer einzigen AWS-Region Instanz bereitgestellt werden. 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 sich die Anwendung mit Ihrer IAM Identity Center-Instanz verbindet und

sich dort 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. Es wird ein Browserfenster 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.

> **Note**
>
> Wenn Sie Kunden verwenden`device.sso.region.amazonaws.com`, müssen Sie Ihren Autorisierungsablauf aktualisieren, um Proof Key for Code Exchange (PKCE) zu

verwenden. Weitere Informationen finden Sie unter Konfiguration der IAM Identity Center-Authentifizierung mit dem AWS CLI im AWS Command Line Interface Benutzerhandbuch.

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 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, und 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, legt der Client die Bereiche fest, in denen die beabsichtigten Aktionen deklariert werden, für die der Benutzer seine Zustimmung geben muss.

OAuth 2.0-Clients verwenden `scope` Werte, wie sie 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	Description	Dienste, die unterstützt werden von
`sso:account:access`	Greifen Sie auf von IAM Identity Center verwaltete Konten und Berechtigungssätze zu.	IAM Identity Center
`codewhisperer:analysis`	Ermöglichen Sie den Zugriff auf die Amazon Q Developer-Codeanalyse.	AWS Builder ID und IAM Identity Center
`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
`verified_access:ap`	Aktivieren AWS Verified Access	AWS Verified Access

Scope	Description	Dienste, die unterstützt werden von
`plication :connect`		
`redshift: connect`	Connect zu Amazon Redshift her	Amazon Redshift
`datazone: domain:access`	Greifen Sie auf Ihre DataZone Domain-Ausführungsrolle zu	Amazon DataZone
`nosqlwork bench:dat amodeladviser`	Datenmodelle erstellen und lesen	NoSQL Workbench
`transform :read_write`	Aktivieren Sie den Zugriff auf AWS Transform Agent für die Codetransformation	AWS Transformation

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 Zugriff auf diese Anwendungen benötigen AWS-Services, 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 weitergeben AWS-Services.

Themen

- Richten Sie eine Anwendung aus dem IAM Identity Center-Anwendungskatalog ein

- Richten Sie Ihre eigene SAML 2.0-Anwendung ein

Richten Sie eine Anwendung aus dem IAM Identity Center-Anwendungskatalog ein

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.

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 aus.
4. Wählen Sie Anwendung hinzufügen.
5. Wählen Sie auf der Seite Anwendungstyp auswählen unter Setup-Präferenz 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 Machen Sie sich mit den Anwendungseigenschaften in der IAM Identity Center-Konsole vertraut.
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 der 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 aus.
4. Wählen Sie Anwendung hinzufügen.
5. Wählen Sie auf der Seite Anwendungstyp auswählen unter Einrichtungspräferenz 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 Machen Sie sich mit den Anwendungseigenschaften in der IAM Identity Center-Konsole vertraut.
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.

Überblick über die Verbreitung vertrauenswürdiger Identitäten

Die Weitergabe vertrauenswürdiger Identitäten ist eine Funktion von IAM Identity Center, mit der Administratoren Berechtigungen auf der Grundlage von AWS-Services Benutzerattributen wie Gruppenzuordnungen gewähren können. Bei der Weitergabe vertrauenswürdiger Identitäten wird einer IAM-Rolle ein Identitätskontext hinzugefügt, um den Benutzer zu identifizieren, der Zugriff AWS auf Ressourcen anfordert. Dieser Kontext wird an andere weitergegeben. AWS-Services

Der Identitätskontext umfasst Informationen, AWS-Services anhand derer Autorisierungsentscheidungen getroffen werden, wenn sie Zugriffsanfragen erhalten. Zu diesen Informationen gehören Metadaten, mit denen der Anforderer (z. B. ein IAM Identity Center-Benutzer), der AWS-Service Zugriff angefordert wird (z. B. Amazon Redshift) und der Zugriffsumfang (z. B. schreibgeschützter Zugriff) identifiziert werden. Der Empfänger AWS-Service verwendet diesen Kontext und alle dem Benutzer zugewiesenen Berechtigungen, um den Zugriff auf seine Ressourcen zu autorisieren.

Vorteile der Verbreitung vertrauenswürdiger Identitäten

Die Weitergabe vertrauenswürdiger Identitäten ermöglicht es den Administratoren von AWS-Services , mithilfe der Unternehmensidentitäten Ihrer Belegschaft Berechtigungen für Ressourcen wie Daten zu erteilen. Darüber hinaus können sie anhand von Serviceprotokollen überprüfen, wer auf welche Daten zugegriffen hat oder AWS CloudTrail. Wenn Sie ein IAM Identity Center-Administrator sind, werden Sie möglicherweise von anderen AWS-Service Administratoren aufgefordert, die Verbreitung vertrauenswürdiger Identitäten zu aktivieren.

Die Verbreitung vertrauenswürdiger Identitäten aktivieren

Das Aktivieren der Verbreitung vertrauenswürdiger Identitäten umfasst die folgenden zwei Schritte:

1. Aktivieren Sie IAM Identity Center und verbinden Sie Ihre bestehende Identitätsquelle mit IAM Identity Center. Sie verwalten die Identitäten Ihrer Belegschaft weiterhin in Ihrer bestehenden Identitätsquelle. Wenn Sie sie mit IAM Identity Center verbinden, wird ein Verweis auf Ihre Belegschaft erstellt, den alle AWS-Services in Ihrem Anwendungsfall gemeinsam nutzen können. Es steht auch Datenbesitzern zur Verfügung, um sie in future Anwendungsfällen zu verwenden.

2. Stellen Sie AWS-Services in Ihrem Anwendungsfall Connect zu IAM Identity Center her — Der Administrator jedes Anwendungsfalls AWS-Service im Trusted Identity Propagation-Anwendungsfall folgt den Anweisungen in der jeweiligen Servicedokumentation, um den Service mit dem IAM Identity Center zu verbinden.

> **Note**
>
> Wenn Ihr Anwendungsfall eine von einem Drittanbieter oder von einem Kunden entwickelte Anwendung umfasst, aktivieren Sie die Verbreitung vertrauenswürdiger Identitäten, indem Sie eine Vertrauensbeziehung zwischen dem Identitätsanbieter, der die Anwendungsbenutzer authentifiziert, und dem IAM Identity Center konfigurieren. Auf diese Weise kann Ihre Anwendung den zuvor beschriebenen Prozess zur Verbreitung vertrauenswürdiger Identitäten nutzen.
> Weitere Informationen finden Sie unter Verwenden Sie Anwendungen mit einem vertrauenswürdigen Token-Emittenten.

So funktioniert die Verbreitung vertrauenswürdiger Identitäten

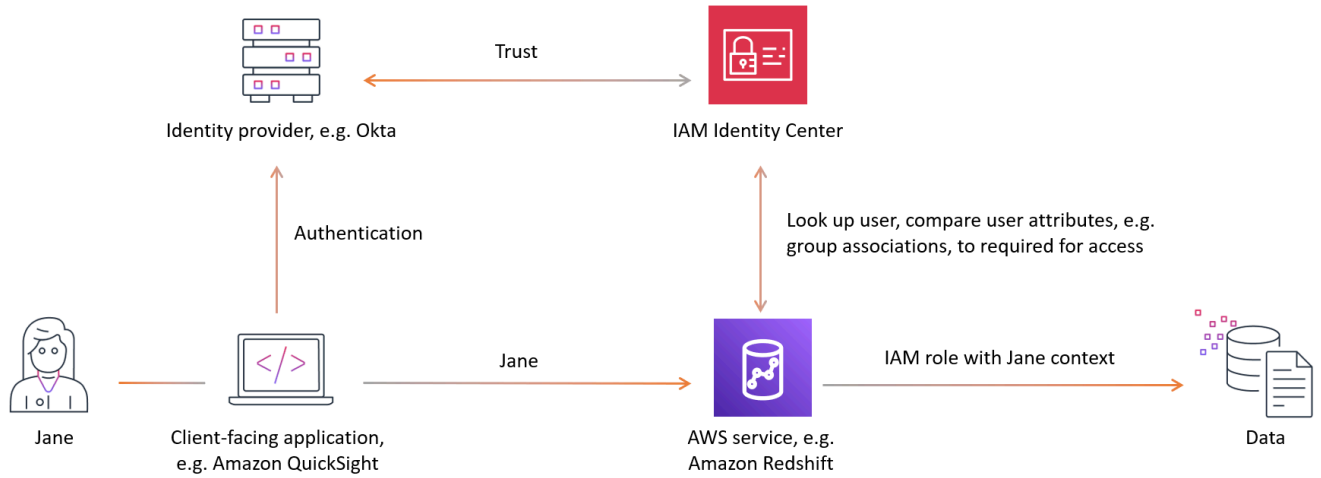
Das folgende Diagramm zeigt den allgemeinen Arbeitsablauf für die Weitergabe vertrauenswürdiger Identitäten:

1. Benutzer authentifizieren sich mit einer clientseitigen Anwendung, beispielsweise Quick Suite.
2. Die clientseitige Anwendung fordert Zugriff zur Verwendung und Abfrage von Daten AWS-Service an und enthält Informationen über den Benutzer.

> **Note**
>
> Einige Anwendungsfälle zur Verbreitung vertrauenswürdiger Identitäten beinhalten Tools, die AWS-Services mithilfe von Diensttreibern interagieren. Ob dies auf Ihren Anwendungsfall zutrifft, erfahren Sie in der Anleitung zu Anwendungsfällen.

3. Das AWS-Service verifiziert die Benutzeridentität mit IAM Identity Center und vergleicht die Benutzerattribute, wie ihre Gruppenzuordnungen, mit denen, die für den Zugriff erforderlich sind. Der AWS-Service autorisiert den Zugriff, solange der Benutzer oder seine Gruppe über die erforderlichen Berechtigungen verfügt.
4. AWS-Services kann die Benutzerkennung in AWS CloudTrail und in ihren Dienstprotokollen protokollieren. Einzelheiten finden Sie in der Servicedokumentation.

Die folgende Abbildung bietet einen Überblick über die zuvor beschriebenen Schritte im Workflow zur Verbreitung vertrauenswürdiger Identitäten:



Themen

- Voraussetzungen und Überlegungen
- Anwendungsfälle zur Verbreitung vertrauenswürdiger Identitäten
- Autorisierungsdienste

Voraussetzungen und Überlegungen

Bevor Sie die Verbreitung vertrauenswürdiger Identitäten einrichten, sollten Sie sich mit den folgenden Voraussetzungen und Überlegungen vertraut machen.

Themen

- Voraussetzungen
- Überlegungen
- Überlegungen zu vom Kunden verwalteten Anwendungen

Voraussetzungen

Um Trusted Identity Propagation zu verwenden, stellen Sie sicher, dass Ihre Umgebung die folgenden Voraussetzungen erfüllt:

- IAM Identity Center aktivieren und bereitstellen
  - Um Trusted Identity Propagation zu verwenden, müssen Sie IAM Identity Center in derselben Umgebung aktivieren, in der auch AWS-Region die AWS Anwendungen und Dienste aktiviert sind, auf die Ihre Benutzer zugreifen werden. Weitere Informationen finden Sie unter IAM Identity Center aktivieren.
    - Die IAM Identity Center-Organisationsinstanz wird empfohlen — Wir empfehlen Ihnen, eine Organisationsinstanz von IAM Identity Center zu verwenden, die Sie im Verwaltungskonto von aktivieren. AWS Organizations Sie können die Verwaltung einer Organisationsinstanz von IAM Identity Center an ein Mitgliedskonto delegieren. Wenn Sie sich für eine Kontoinstanz von IAM Identity Center entscheiden, muss sich alles AWS-Services , worauf Benutzer mit Trusted Identity Propagation zugreifen können, in derselben AWS-Konto Instanz befinden, in der Sie IAM Identity Center aktivieren. Weitere Informationen finden Sie unter Kontoinstanzen von IAM Identity Center.
  - Connect Sie Ihren bestehenden Identitätsanbieter mit IAM Identity Center und stellen Sie Ihre Benutzer und Gruppen in IAM Identity Center bereit. Weitere Informationen finden Sie unter Tutorials zu Identitätsquellen im IAM Identity Center.
- Connect die AWS verwalteten Anwendungen und Dienste in Ihrem Anwendungsfall zur Verbreitung vertrauenswürdiger Identitäten mit dem IAM Identity Center. Um Trusted Identity Propagation nutzen zu können, müssen AWS verwaltete Anwendungen mit IAM Identity Center verbunden sein.

Überlegungen

Beachten Sie bei der Konfiguration und Verwendung von Trusted Identity Propagation die folgenden Überlegungen:

- Organisation und Kontoinstanz von IAM Identity Center
  - Eine Organisationsinstanz von IAM Identity Center bietet Ihnen die größtmögliche Kontrolle und Flexibilität, um Ihre Anwendungsfälle auf mehrere Benutzer und AWS-Konten auszuweiten. AWS-Services Wenn Sie keine Organisationsinstanz verwenden können, wird Ihr Anwendungsfall möglicherweise mit Kontoinstanzen von IAM Identity Center unterstützt. Weitere Informationen darüber, welche Kontoinstanzen von IAM Identity Center AWS-Services in Ihrem

Anwendungsfall unterstützt werden, finden Sie unter. AWS verwaltete Anwendungen, die Sie mit IAM Identity Center verwenden können

- 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.

Überlegungen zu vom Kunden verwalteten Anwendungen

Ihre Belegschaft kann von der Verbreitung vertrauenswürdiger Identitäten profitieren, auch wenn Ihre Benutzer beispielsweise mit kundenorientierten Anwendungen interagieren, die nicht von Ihnen verwaltet werden AWS, Tableau oder Ihren individuell entwickelten Anwendungen. Die Benutzer dieser Anwendungen werden möglicherweise nicht im IAM Identity Center bereitgestellt. Um eine reibungslose Erkennung und Autorisierung des Benutzerzugriffs auf AWS Ressourcen zu ermöglichen, können Sie mit IAM Identity Center eine vertrauenswürdige Beziehung zwischen dem Identitätsanbieter, der Ihre Benutzer authentifiziert, und IAM Identity Center einrichten. Weitere Informationen finden Sie unter Verwenden Sie Anwendungen mit einem vertrauenswürdigen Token-Emittenten.

Darüber hinaus erfordert die Konfiguration der Verbreitung vertrauenswürdiger Identitäten für Ihre Anwendung:

- Ihre Anwendung muss das OAuth 2.0-Framework für die Authentifizierung verwenden. Die Verbreitung vertrauenswürdiger Identitäten unterstützt keine SAML 2.0-Integrationen.
- Ihre Anwendung muss vom IAM Identity Center erkannt werden. Folgen Sie den Anweisungen, die für Ihren Anwendungsfall spezifisch sind.

Anwendungsfälle zur Verbreitung vertrauenswürdiger Identitäten

Als IAM Identity Center-Administrator werden Sie möglicherweise gebeten, bei der Konfiguration der Weitergabe vertrauenswürdiger Identitäten von benutzerseitigen Anwendungen an zu helfen. AWS-Services Um diese Anfrage zu unterstützen, benötigen Sie die folgenden Informationen:

- Mit welcher kundenorientierten Anwendung werden Ihre Benutzer interagieren?
- Welche AWS-Services werden verwendet, um die Daten abzufragen und den Zugriff auf die Daten zu autorisieren?

- Was AWS-Service autorisiert den Zugriff auf die Daten?

Ihre Rolle bei der Aktivierung von Anwendungsfällen zur Verbreitung vertrauenswürdiger Identitäten, bei denen keine Drittanbieteranwendungen oder speziell entwickelte Anwendungen involviert sind, besteht darin,

1. Aktivieren Sie IAM Identity Center.
2. Connect Sie Ihre bestehende Identitätsquelle mit dem IAM Identity Center.

Die verbleibenden Schritte der Konfiguration vertrauenswürdiger Identitäten für diese Anwendungsfälle werden innerhalb der verbundenen Anwendungen AWS-Services und Anwendungen ausgeführt. Die Administratoren der verbundenen Anwendungen AWS-Services oder Anwendungen sollten in den jeweiligen Benutzerhandbüchern nach umfassenden dienstspezifischen Anleitungen suchen.

Ihre Rolle bei der Aktivierung von Anwendungsfällen zur Verbreitung vertrauenswürdiger Identitäten, an denen Drittanbieteranwendungen oder speziell entwickelte Anwendungen beteiligt sind, umfasst die Schritte zum Herstellen IAM Identity Center aktivieren und Verbinden Ihrer Identitätsquelle sowie:

1. Konfiguration der Verbindung Ihres Identitätsanbieters (IdP) mit dem Drittanbieter oder der individuell entwickelten Anwendung.
2. Aktivierung der Erkennung der Drittanbieteranwendung oder der kundenspezifisch entwickelten Anwendung durch IAM Identity Center
3. Konfiguration Ihres IdP als vertrauenswürdigen Token-Aussteller im IAM Identity Center. Weitere Informationen finden Sie unter Verwenden Sie Anwendungen mit einem vertrauenswürdigen Token-Emittenten.

Die Administratoren der verbundenen Anwendungen AWS-Services sollten sich an die jeweiligen Benutzerhandbücher halten, um umfassende dienstspezifische Anleitungen zu erhalten.

Anwendungsfälle für Analytik, Data Lakehouse und maschinelles Lernen

Sie können Trusted Propagation-Anwendungsfälle mit den folgenden Analyse- und Machine-Learning-Diensten aktivieren:

- Amazon Redshift — Anleitungen finden Sie unterVertrauenswürdige Identitätsverbreitung mit Amazon Redshift.

- Amazon EMR — Anleitungen finden Sie unterVertrauenswürdige Identitätsverbreitung mit Amazon EMR.
- Amazon Athena — Anleitungen finden Sie unterVertrauenswürdige Identitätsverbreitung mit Amazon Athena.
- SageMaker Studio — Anleitungen finden Sie unterVertrauenswürdige Identitätsverbreitung mit Amazon SageMaker Studio.

Zusätzliche Anwendungsfälle

Sie können IAM Identity Center und die Verbreitung vertrauenswürdiger Identitäten mit folgenden zusätzlichen AWS-Services Optionen aktivieren:

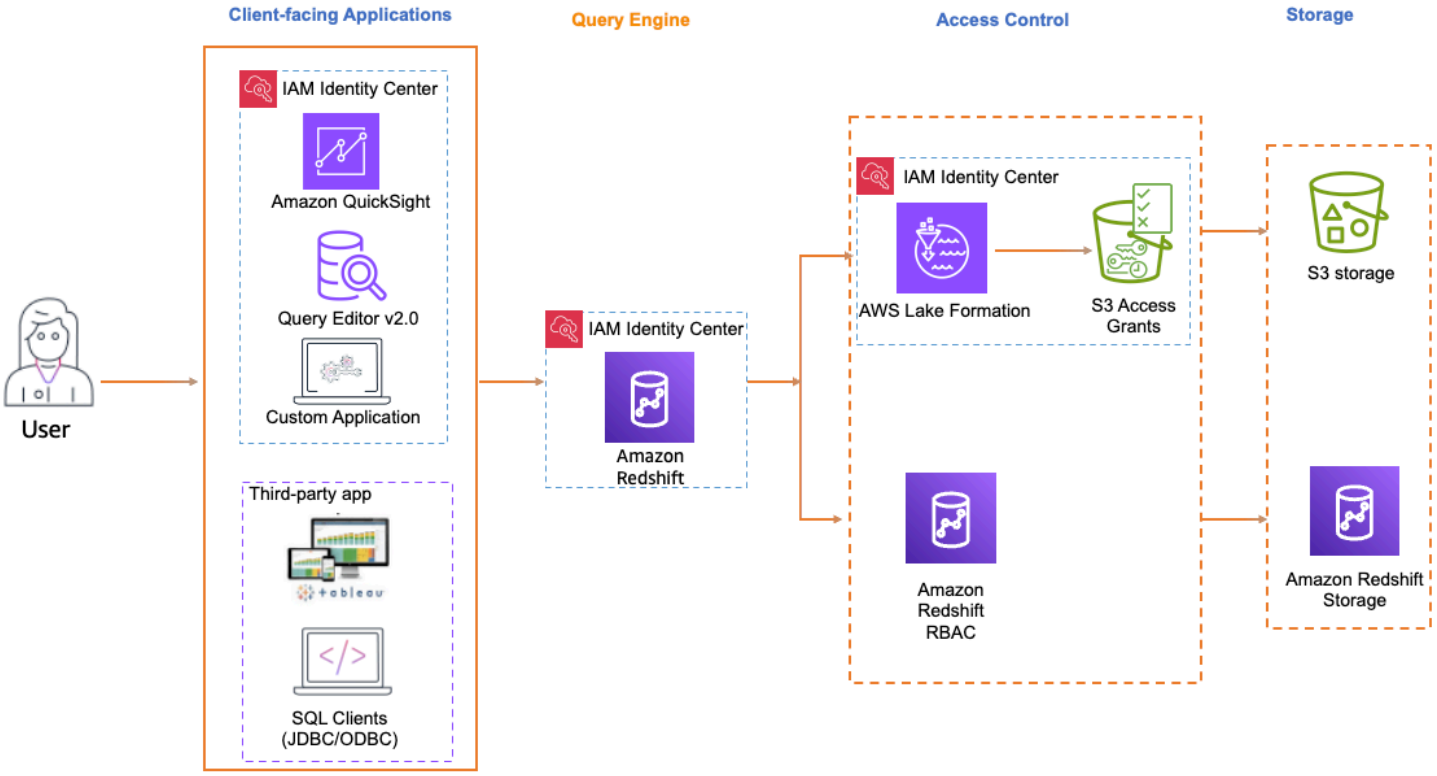
- Amazon Q Business — Anleitungen finden Sie unter:
  - Administrator-Workflow für Apps, die IAM Identity Center verwenden.
  - Konfiguration einer Amazon Q Business-Anwendung mithilfe von IAM Identity Center.
  - Konfigurieren Sie Amazon Q Business mit IAM Identity Center Trusted Identity Propagation.
- Amazon OpenSearch Service — Anleitungen finden Sie unter:
  - Support für vertrauenswürdige Identitätsverbreitung durch IAM Identity Center für Amazon OpenSearch Service.
  - Zentralisierte OpenSearch Benutzeroberfläche (Dashboards) mit Amazon OpenSearch Service.
- AWS Transfer Family- Anleitungen finden Sie unter:
  - Transfer Family Familien-Web-Apps.

Themen

Vertrauenswürdige Identitätsverbreitung mit Amazon Redshift

Die Schritte zur Aktivierung der Verbreitung vertrauenswürdiger Identitäten hängen davon ab, ob Ihre Benutzer mit AWS verwalteten Anwendungen oder mit kundenverwalteten Anwendungen

interagieren. Das folgende Diagramm zeigt eine Konfiguration zur Weitergabe vertrauenswürdiger Identitäten für clientseitige Anwendungen — entweder AWS verwaltet oder extern AWS —, die Amazon Redshift-Daten mit Zugriffskontrolle abfragen, die entweder von Amazon Redshift oder von Autorisierungsdiensten wie AWS Lake Formation Amazon S3 bereitgestellt wird. Access Grants



Wenn die Weitergabe vertrauenswürdiger Identitäten an Amazon Redshift aktiviert ist, können Redshift-Administratoren Redshift so konfigurieren, dass automatisch Rollen für IAM Identity Center als Identitätsanbieter erstellt, Redshift-Rollen Gruppen in IAM Identity Center zugeordnet werden und die rollenbasierte Zugriffskontrolle von Redshift verwendet wird, um Zugriff zu gewähren.

Unterstützte clientseitige Anwendungen

AWS verwaltete Anwendungen

Die folgenden AWS verwalteten clientseitigen Anwendungen unterstützen die Weitergabe vertrauenswürdiger Identitäten an Amazon Redshift:

- Amazon Redshift Query Editor V2
- Quick Suite

> **Note**
>
> Wenn Sie Amazon Redshift Spectrum für den Zugriff auf externe Datenbanken oder Tabellen verwenden AWS Glue Data Catalog, sollten Sie die Einrichtung von Lake Formation und Amazon S3 in Betracht ziehen, Access Grants um eine detaillierte Zugriffskontrolle zu ermöglichen.

Vom Kunden verwaltete Anwendungen

Die folgenden vom Kunden verwalteten Anwendungen unterstützen die Weitergabe vertrauenswürdiger Identitäten an Amazon Redshift:

- Tableaueinschließlich Tableau Desktop TableauServer, und Tableau Prep
  - Informationen zur Aktivierung der Verbreitung vertrauenswürdiger Identitäten für Benutzer von Tableau finden Sie unter Integrieren Tableau und Okta mit Amazon Redshift using IAM Identity Center im AWS Big Data-Blog.
- SQL-Clients (DBeaverund) DBVisualizer
  - Informationen zur Aktivierung der Verbreitung vertrauenswürdiger Identitäten für Benutzer von SQL Clients (DBeaverundDBVisualizer) finden Sie unter Integrate Identity Provider (IdP) with Amazon Redshift Query Editor V2 und SQL Client using IAM Identity Center for seamless Single Sign-On im AWS Big Data-Blog.

Einrichtung der Verbreitung vertrauenswürdiger Identitäten mit Amazon Redshift Query Editor V2

Das folgende Verfahren führt Sie durch die Schritte zur Weitergabe vertrauenswürdiger Identitäten von Amazon Redshift Query Editor V2 zu Amazon Redshift.

Voraussetzungen

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

1. Aktivieren Sie IAM Identity Center. Eine Organisationsinstanz wird empfohlen. Weitere Informationen finden Sie unter Voraussetzungen und Überlegungen.
2. Stellen Sie die Benutzer und Gruppen aus Ihrer Identitätsquelle im IAM Identity Center bereit.

Die Aktivierung der Verbreitung vertrauenswürdiger Identitäten umfasst Aufgaben, die von einem IAM Identity Center-Administrator in der IAM Identity Center-Konsole ausgeführt werden, und Aufgaben,

die von einem Amazon Redshift Redshift-Administrator in der Amazon Redshift Redshift-Konsole ausgeführt werden.

Vom IAM Identity Center-Administrator ausgeführte Aufgaben

Die folgenden Aufgaben mussten vom IAM Identity Center-Administrator erledigt werden:

1. Erstellen Sie eine IAM-Rolle in dem Konto, in dem der Amazon Redshift Redshift-Cluster oder die Serverless-Instance vorhanden ist, mit der folgenden Berechtigungsrichtlinie. Weitere Informationen finden Sie unter IAM-Rollenerstellung.

   - Die folgenden Richtlinienbeispiele enthalten die erforderlichen Berechtigungen, um dieses Tutorial abzuschließen. Um diese Richtlinie zu verwenden, ersetzen Sie die Richtlinie *italicized placeholder text* im Beispiel durch Ihre eigenen Informationen. Weitere Anweisungen finden Sie unter Richtlinie erstellen oder Richtlinie bearbeiten.

     Genehmigungsrichtlinie:

     JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRedshiftApplication",
            "Effect": "Allow",
            "Action": [
                "redshift:DescribeQev2IdcApplications",
                "redshift-serverless:ListNamespaces",
                "redshift-serverless:ListWorkgroups",
                "redshift-serverless:GetWorkgroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowIDCPermissions",
            "Effect": "Allow",
            "Action": [
                "sso:DescribeApplication",
                "sso:DescribeInstance"
            ],
            "Resource": [
```

```
                "arn:aws:sso:::instance/Your-IAM-Identity-Center-Instance
 ID",
                "arn:aws:sso::111122223333:application/Your-IAM-Identity-
Center-Instance-ID/*"
            ]
        }
    ]
}
```

Vertrauensrichtlinie:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "redshift-serverless.amazonaws.com",
                    "redshift.amazonaws.com"
                ]
            },
            "Action": [
                "sts:AssumeRole",
                "sts:SetContext"
            ]
        }
    ]
}
```

2. Erstellen Sie einen Berechtigungssatz in dem AWS Organizations Verwaltungskonto, in dem IAM Identity Center aktiviert ist. Sie werden es im nächsten Schritt verwenden, um Verbundbenutzern den Zugriff auf Redshift Query Editor V2 zu ermöglichen.

   a. Gehen Sie zur IAM Identity Center-Konsole und wählen Sie unter Berechtigungen für mehrere Konten die Option Berechtigungssätze aus.

   b. Wählen Sie Create permission set (Berechtigungssatz erstellen) aus.

c. Wählen Sie Benutzerdefinierter Berechtigungssatz und dann Weiter.

d. Wählen Sie unter AWS Verwaltete Richtlinien die Option aus **`AmazonRedshiftQueryEditorV2ReadSharing`**.

e. Fügen Sie unter Inline-Richtlinie die folgende Richtlinie hinzu:

JSON

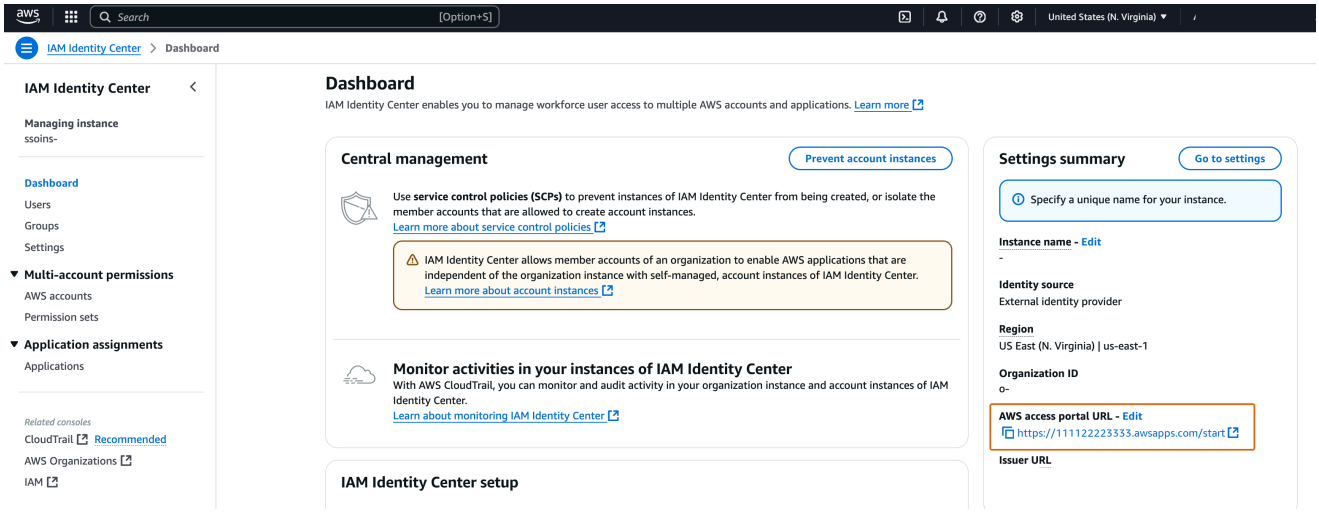
```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "redshift:DescribeQev2IdcApplications",
                "redshift-serverless:ListNamespaces",
                "redshift-serverless:ListWorkgroups",
                "redshift-serverless:GetWorkgroup"
            ],
            "Resource": "*"
        }
    ]
}
```

f. Wählen Sie Weiter aus und geben Sie dann einen Namen für den Namen des Berechtigungssatzes ein. Beispiel, **`Redshift-Query-Editor-V2`**.

g. Legen Sie unter Relaystatus — optional den Standard-Relaystatus auf die URL des Query-Editors V2 fest und verwenden Sie dabei das folgende Format:`https://`*`your-region`*`.console.aws.amazon.com/sqlworkbench/home`.

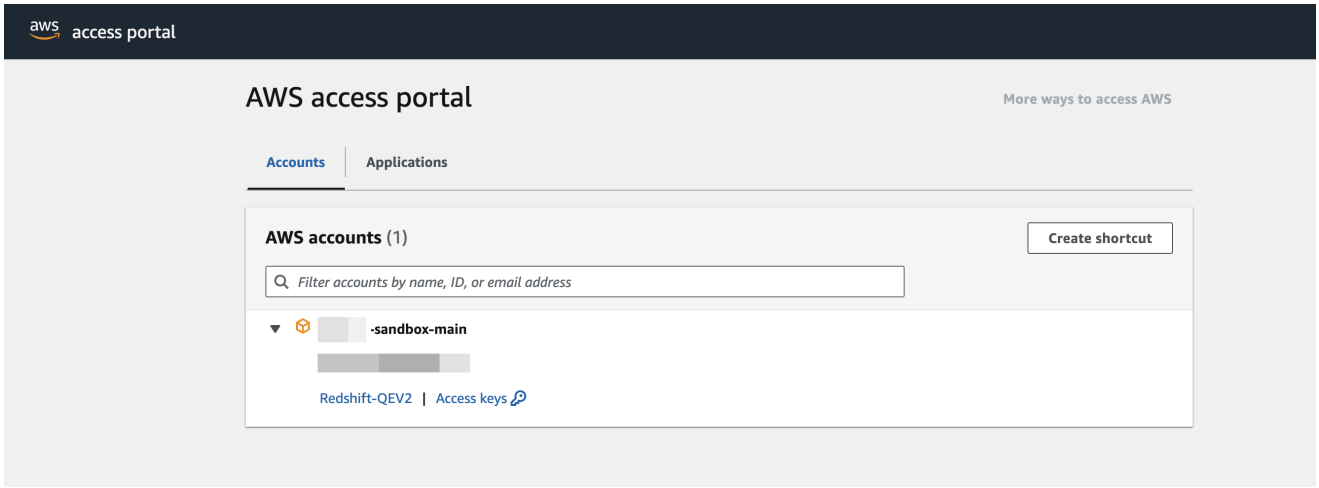
h. Überprüfen Sie die Einstellungen und wählen Sie Erstellen aus.

i. Navigieren Sie zum IAM Identity Center Dashboard und kopieren Sie die URL des AWS Zugriffsportals aus dem Abschnitt „Zusammenfassung der Einstellungen“.



j. Öffnen Sie ein neues Inkognito-Browserfenster und fügen Sie die URL ein.

Dadurch gelangen Sie zu Ihrem AWS Zugriffsportal und stellen sicher, dass Sie sich mit einem IAM Identity Center-Benutzer anmelden.



Weitere Informationen zum Berechtigungssatz finden Sie unterAWS-Konten Mit Berechtigungssätzen verwalten.

3. Ermöglichen Sie Verbundbenutzern den Zugriff auf Redshift Query Editor V2.

a. Öffnen Sie im AWS Organizations Verwaltungskonto die IAM Identity Center-Konsole.

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

c. Wählen Sie auf der AWS-Konten Seite die aus AWS-Konto , der Sie Zugriff zuweisen möchten.

d. Wählen Sie Benutzer oder Gruppen zuweisen aus.

e. Wählen Sie auf der Seite Benutzer und Gruppen zuweisen die Benutzer und/oder Gruppen aus, für die Sie den Berechtigungssatz erstellen möchten. Wählen Sie anschließend Weiter.

f. Wählen Sie auf der Seite „Berechtigungssätze zuweisen“ den Berechtigungssatz aus, den Sie im vorherigen Schritt erstellt haben. Wählen Sie anschließend Weiter.

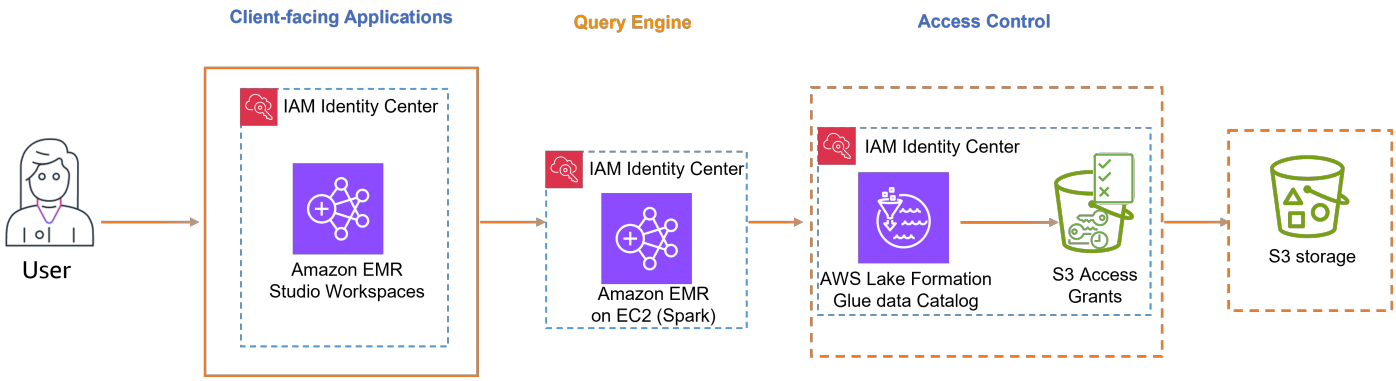
g. Überprüfen Sie auf der Seite Aufgaben überprüfen und einreichen Ihre Auswahl und wählen Sie Absenden.

Von einem Amazon Redshift Redshift-Administrator ausgeführte Aufgaben

Um die Weitergabe vertrauenswürdiger Identitäten an Amazon Redshift zu aktivieren, muss ein Amazon Redshift-Clusteradministrator oder Amazon Redshift Serverless-Administrator eine Reihe von Aufgaben in der Amazon Redshift Redshift-Konsole ausführen. Weitere Informationen finden Sie im Big Data-Blog unter Integrieren von Identity Provider (IdP) in Amazon Redshift Query Editor V2 und SQL Client using IAM Identity Center for Seamless Single Sign-On.AWS

Vertrauenswürdige Identitätsverbreitung mit Amazon EMR

Das folgende Diagramm zeigt eine Konfiguration zur Weitergabe vertrauenswürdiger Identitäten für Amazon EMR Studio unter Verwendung von Amazon EMR auf Amazon EC2 mit Zugriffskontrolle von AWS Lake Formation und Amazon S3. Access Grants



Unterstützte clientseitige Anwendungen

- Amazon EMR Studio

Gehen Sie wie folgt vor, um die Verbreitung vertrauenswürdiger Identitäten zu aktivieren:

- Richten Sie Amazon EMR Studio als clientseitige Anwendung für den Amazon EMR-Cluster ein.
- Richten Sie Amazon EMR Cluster auf Amazon ein EC2 mit Apache Spark.

- Empfohlen: AWS Lake Formationund Amazon S3 Access Grants, um eine differenzierte Zugriffskontrolle auf AWS Glue Data Catalog und die zugrunde liegenden Datenspeicherorte in S3 zu ermöglichen.

Einrichtung der Verbreitung vertrauenswürdiger Identitäten mit Amazon EMR Studio

Das folgende Verfahren führt Sie durch die Einrichtung von Amazon EMR Studio für die Weitergabe vertrauenswürdiger Identitäten in Abfragen gegen laufende Amazon Athena Athena-Arbeitsgruppen oder Amazon EMR-Cluster. Apache Spark

Voraussetzungen

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

1. Aktivieren Sie IAM Identity Center. Eine Organisationsinstanz wird empfohlen. Weitere Informationen finden Sie unter Voraussetzungen und Überlegungen.
2. Stellen Sie die Benutzer und Gruppen aus Ihrer Identitätsquelle im IAM Identity Center bereit.

Um die Einrichtung der vertrauenswürdigen Identitätsverbreitung von Amazon EMR Studio abzuschließen, muss der EMR Studio-Administrator die folgenden Schritte ausführen.

Schritt 1. Erstellen Sie die erforderlichen IAM-Rollen für EMR Studio

In diesem Schritt erstellt der Amazon Studio EMR-Administrator eine IAM-Servicerolle und eine IAM-Benutzerrolle für EMR. Studio

1. Eine EMR Studio-Servicerolle erstellen — EMR Studio übernimmt diese IAM-Rolle, um Workspaces und Notebooks sicher zu verwalten, Verbindungen zu Clustern herzustellen und Dateninteraktionen abzuwickeln.

   a. Navigieren Sie zur IAM-Konsole (https://console.aws.amazon.com/iam/) und erstellen Sie eine IAM-Rolle.

   b. Wählen Sie AWS-Serviceals vertrauenswürdige Entität und dann Amazon EMR aus. Fügen Sie die folgenden Richtlinien hinzu, um die Berechtigungen und das Vertrauensverhältnis der Rolle zu definieren.

      Um diese Richtlinie zu verwenden, ersetzen Sie die Richtlinie *`italicized placeholder text`* im Beispiel durch Ihre eigenen Informationen. Weitere Anweisungen finden Sie unter Richtlinie erstellen oder Richtlinie bearbeiten.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ObjectActions",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::Your-S3-Bucket-For-EMR-Studio/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "Your-AWS-Account-ID"
                }
            }
        },
        {
            "Sid": "BucketActions",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetEncryptionConfiguration"
            ],
            "Resource": [
                "arn:aws:s3:::Your-S3-Bucket-For-EMR-Studio"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "Your-AWS-Account-ID"
                }
            }
        }
    ]
}
```

Eine Referenz aller Servicerollenberechtigungen finden Sie unter EMR Studio-Servicerollenberechtigungen.

2. Eine EMR Studio-Benutzerrolle für die IAM Identity Center-Authentifizierung erstellen — EMR Studio übernimmt diese Rolle, wenn sich ein Benutzer über IAM Identity Center anmeldet, um Workspaces, EMR-Cluster, Jobs und Git-Repositorys zu verwalten. Diese Rolle wird verwendet, um den Workflow zur Verbreitung vertrauenswürdiger Identitäten zu initiieren.

> **Note**
>
> Die EMR Studio-Benutzerrolle muss keine Berechtigungen für den Zugriff auf die Amazon S3 S3-Speicherorte der Tabellen im AWS Glue Katalog enthalten. AWS Lake Formation Berechtigungen und registrierte Standorte an Seen werden verwendet, um temporäre Berechtigungen zu erhalten.

Die folgende Beispielrichtlinie kann in einer Rolle verwendet werden, die es einem Benutzer von EMR Studio ermöglicht, Athena-Arbeitsgruppen zum Ausführen von Abfragen zu verwenden.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDefaultEC2SecurityGroupsCreationInVPCWithEMRTags",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSecurityGroup"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:vpc/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/for-use-with-amazon-emr-managed-
policies": "true"
                }
            }
```

```
        },
        {
            "Sid": "AllowAddingEMRTagsDuringDefaultSecurityGroupCreation",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/for-use-with-amazon-emr-managed-
policies": "true",
                    "ec2:CreateAction": "CreateSecurityGroup"
                }
            }
        },
        {
            "Sid": "AllowSecretManagerListSecrets",
            "Action": [
                "secretsmanager:ListSecrets"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Sid": "AllowSecretCreationWithEMRTagsAndEMRStudioPrefix",
            "Effect": "Allow",
            "Action": "secretsmanager:CreateSecret",
            "Resource": "arn:aws:secretsmanager:*:*:secret:emr-studio-*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/for-use-with-amazon-emr-managed-
policies": "true"
                }
            }
        },
        {
            "Sid": "AllowAddingTagsOnSecretsWithEMRStudioPrefix",
            "Effect": "Allow",
            "Action": "secretsmanager:TagResource",
            "Resource": "arn:aws:secretsmanager:*:*:secret:emr-studio-*"
        },
        {
            "Sid": "AllowPassingServiceRoleForWorkspaceCreation",
```

```
            "Action": "iam:PassRole",
            "Resource": [
                "arn:aws:iam::111122223333:role/service-
role/AmazonEMRStudio_ServiceRole_Name"
            ],
            "Effect": "Allow"
        },
        {
            "Sid": "AllowS3ListAndLocationPermissions",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::*",
            "Effect": "Allow"
        },
        {
            "Sid": "AllowS3ReadOnlyAccessToLogs",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::aws-logs-Your-AWS-Account-ID-Region/
elasticmapreduce/*"
            ],
            "Effect": "Allow"
        },
        {
            "Sid": "AllowAthenaQueryExecutions",
            "Effect": "Allow",
            "Action": [
                "athena:StartQueryExecution",
                "athena:GetQueryExecution",
                "athena:GetQueryResults",
                "athena:StopQueryExecution",
                "athena:ListQueryExecutions",
                "athena:GetQueryResultsStream",
                "athena:ListWorkGroups",
                "athena:GetWorkGroup",
                "athena:CreatePreparedStatement",
                "athena:GetPreparedStatement",
                "athena:DeletePreparedStatement"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid": "AllowGlueSchemaManipulations",
            "Effect": "Allow",
            "Action": [
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:GetTable",
                "glue:GetTables",
                "glue:GetPartition",
                "glue:GetPartitions"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowQueryEditorToAccessWorkGroup",
            "Effect": "Allow",
            "Action": "athena:GetWorkGroup",
            "Resource": "arn:aws:athena:*:111122223333:workgroup*"
        },
        {
            "Sid": "AllowConfigurationForWorkspaceCollaboration",
            "Action": [
                "elasticmapreduce:UpdateEditor",
                "elasticmapreduce:PutWorkspaceAccess",
                "elasticmapreduce:DeleteWorkspaceAccess",
                "elasticmapreduce:ListWorkspaceAccessIdentities"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "elasticmapreduce:ResourceTag/creatorUserId":
"${aws:userId}"
                }
            }
        },
        {
            "Sid": "DescribeNetwork",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
```

```
                "ec2:DescribeSecurityGroups"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ListIAMRoles",
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AssumeRole",
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": "*"
        }
    ]
}
```

Die folgende Vertrauensrichtlinie ermöglicht es EMR Studio, die Rolle zu übernehmen:

> **Note**
>
> Für die Nutzung von EMR Studio Workspaces und EMR Notebooks sind zusätzliche Berechtigungen erforderlich. Weitere Informationen finden Sie unter Erstellen von Berechtigungsrichtlinien für EMR Studio-Benutzer.

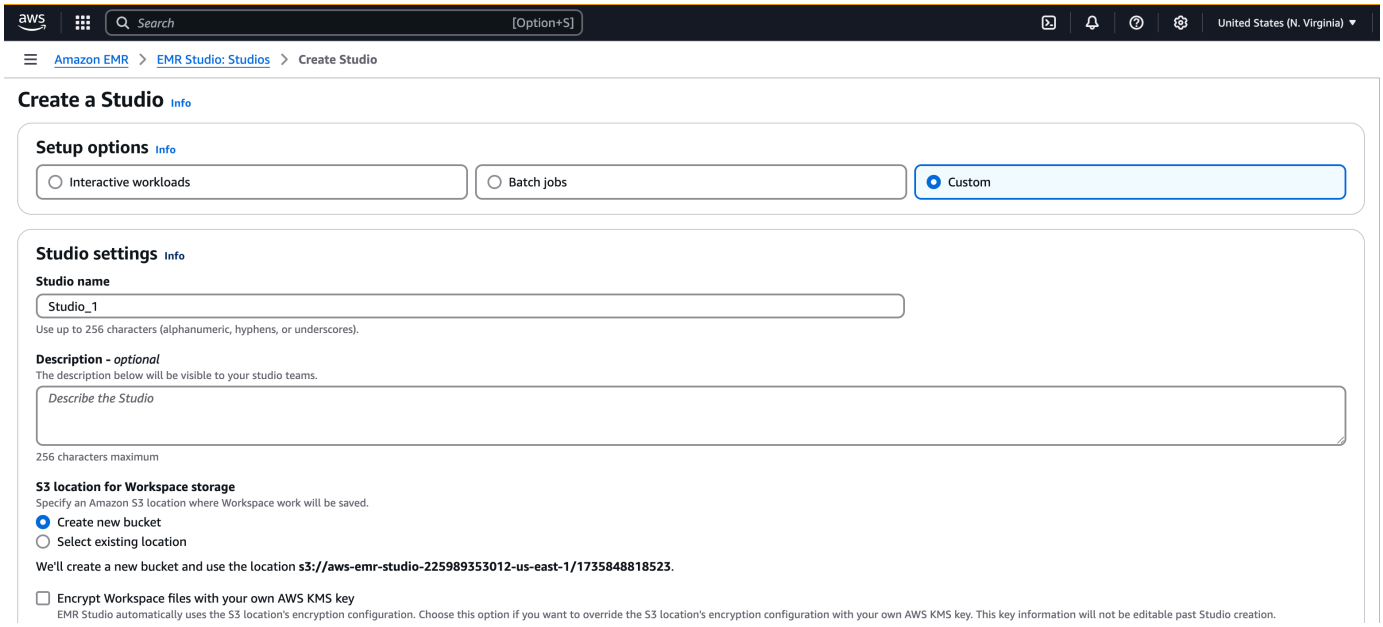
Weitere Informationen finden Sie unter den folgenden Links:

- Benutzerdefinierte IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien definieren
- Berechtigungen für EMR Studio-Dienstrollen

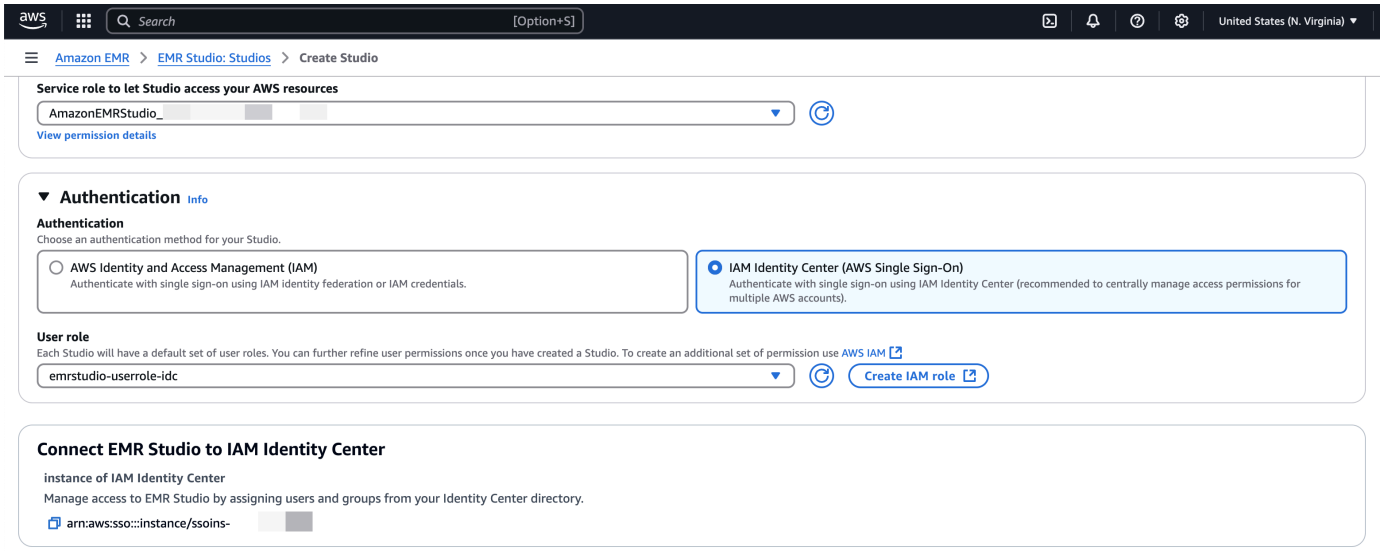
Schritt 2. Erstellen und konfigurieren Sie Ihr EMR Studio

In diesem Schritt erstellen Sie ein Amazon EMR Studio in der EMR Studio-Konsole und verwenden die IAM-Rollen, in denen Sie es erstellt haben. Schritt 1. Erstellen Sie die erforderlichen IAM-Rollen für EMR Studio

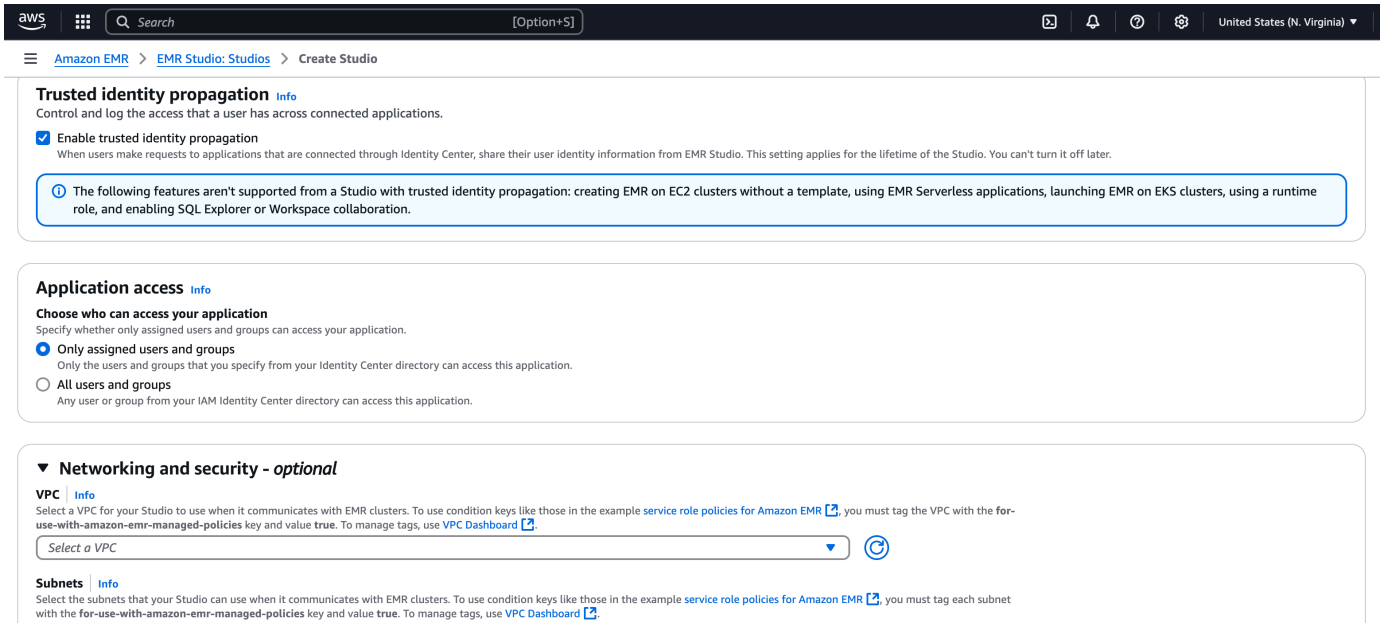
1. Navigieren Sie zur EMR Studio-Konsole, wählen Sie Create Studio und die Option Custom Setup aus. Sie können entweder einen neuen S3-Bucket erstellen oder einen vorhandenen Bucket verwenden. Sie können das Kästchen aktivieren, um Workspace-Dateien mit Ihren eigenen KMS-Schlüsseln zu verschlüsseln. Weitere Informationen finden Sie unter AWS Key Management Service.



2. Wählen Sie unter Servicerolle, damit Studio auf Ihre Ressourcen zugreifen kann, die in erstellte Servicerolle Schritt 1. Erstellen Sie die erforderlichen IAM-Rollen für EMR Studio aus dem Menü aus.
3. Wählen Sie unter Authentifizierung die Option IAM Identity Center aus. Wählen Sie die Benutzerrolle aus, die in Schritt 1. Erstellen Sie die erforderlichen IAM-Rollen für EMR Studio erstellt wurde.



4. Markieren Sie das Kästchen Vertrauenswürdige Identitätsverbreitung. Wählen Sie im Abschnitt Anwendungszugriff die Option Nur zugewiesene Benutzer und Gruppen aus, sodass Sie nur autorisierten Benutzern und Gruppen Zugriff auf dieses Studio gewähren können.
5. (Optional) — Sie können VPC und Subnetz konfigurieren, wenn Sie dieses Studio mit EMR-Clustern verwenden.



6. Überprüfen Sie alle Details und wählen Sie Create Studio aus.
7. Melden Sie sich nach der Konfiguration eines Athena WorkGroup - oder EMR-Clusters mit der Studio-URL an, um:

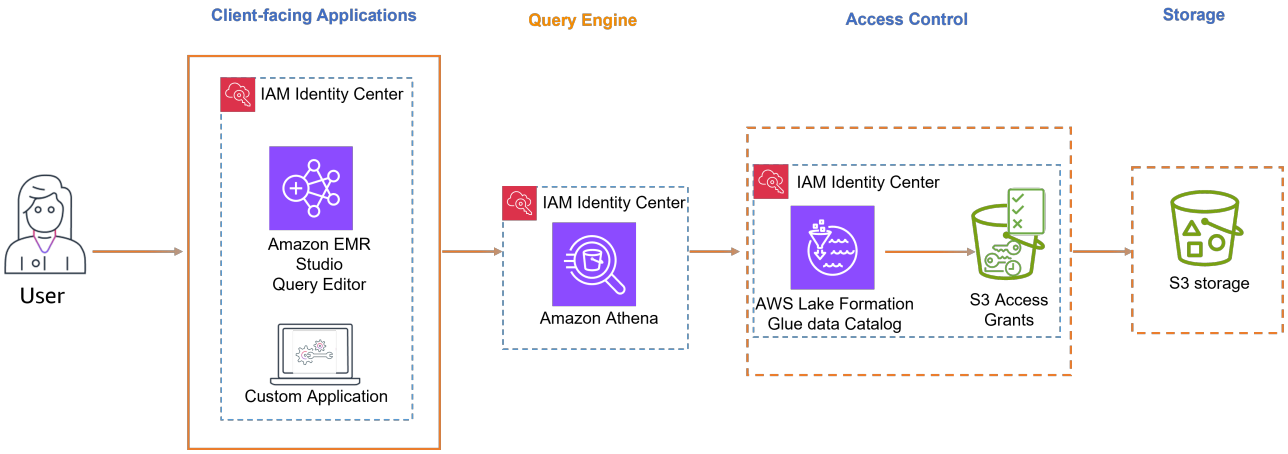
   a. Führen Sie Athena-Abfragen mit dem Abfrage-Editor aus.

b. Führen Sie Spark-Jobs im Workspace mithilfe von Jupyter Notebook aus.

Vertrauenswürdige Identitätsverbreitung mit Amazon Athena

Die Schritte zur Aktivierung der Verbreitung vertrauenswürdiger Identitäten hängen davon ab, ob Ihre Benutzer mit AWS verwalteten Anwendungen oder mit kundenverwalteten Anwendungen interagieren. Das folgende Diagramm zeigt eine Konfiguration zur Weitergabe vertrauenswürdiger Identitäten für clientseitige Anwendungen — entweder AWS verwaltet oder extern AWS —, die Amazon Athena verwenden, um Amazon S3-Daten mit der von Amazon S3 bereitgestellten AWS Lake Formation Zugriffskontrolle abzufragen. Access Grants

> **Note**
>
> - Die Verbreitung vertrauenswürdiger Identitäten mit Amazon Athena erfordert die Verwendung von Trino.
> - Apache Spark- und SQL-Clients, die über ODBC- und JDBC-Treiber mit Amazon Athena verbunden sind, werden nicht unterstützt.



AWS verwaltete Anwendungen

Die folgende AWS verwaltete, clientseitige Anwendung unterstützt die Verbreitung vertrauenswürdiger Identitäten mit Athena:

- Amazon EMR Studio

Gehen Sie wie folgt vor, um die Verbreitung vertrauenswürdiger Identitäten zu aktivieren:

- Richten Sie Amazon EMR Studio als clientseitige Anwendung für Athena ein. Der Abfrage-Editor in EMR Studio wird benötigt, um Athena-Abfragen auszuführen, wenn die Weitergabe vertrauenswürdiger Identitäten aktiviert ist.
- Richten Sie die Athena Workgroup ein.
- Richten Sie AWS Lake Formation es so ein, dass eine differenzierte Zugriffskontrolle für AWS Glue Tabellen auf der Grundlage des Benutzers oder der Gruppe in IAM Identity Center ermöglicht wird.
- Richten Sie Amazon S3 einAccess Grants, um den temporären Zugriff auf die zugrunde liegenden Datenspeicherorte in S3 zu ermöglichen.

> **Note**
>
> Sowohl Lake Formation als auch Amazon S3 Access Grants sind für die Zugriffskontrolle auf AWS Glue Data Catalog und für Athena-Abfrageergebnisse in Amazon S3 erforderlich.

Vom Kunden verwaltete Anwendungen

Informationen zur Aktivierung der Verbreitung vertrauenswürdiger Identitäten für Benutzer von kundenspezifisch entwickelten Anwendungen finden Sie unter AWS-Services Programmgesteuerter Zugriff mithilfe vertrauenswürdiger Identitätsverbreitung im AWS Sicherheitsblog.

Einrichtung der Verbreitung vertrauenswürdiger Identitäten mit Amazon Athena Athena-Arbeitsgruppen

Das folgende Verfahren führt Sie durch die Einrichtung von Amazon Athena Athena-Arbeitsgruppen für die Verbreitung vertrauenswürdiger Identitäten.

Voraussetzungen

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

1. Aktivieren Sie IAM Identity Center. Eine Organisationsinstanz wird empfohlen. Weitere Informationen finden Sie unter Voraussetzungen und Überlegungen.
2. Stellen Sie die Benutzer und Gruppen aus Ihrer Identitätsquelle im IAM Identity Center bereit.
3. Für diese Konfiguration sind Amazon EMR Studio und Amazon S3 Access Grants erforderlich. AWS Lake Formation

Vertrauenswürdige Identitätsverbreitung mit Athena einrichten

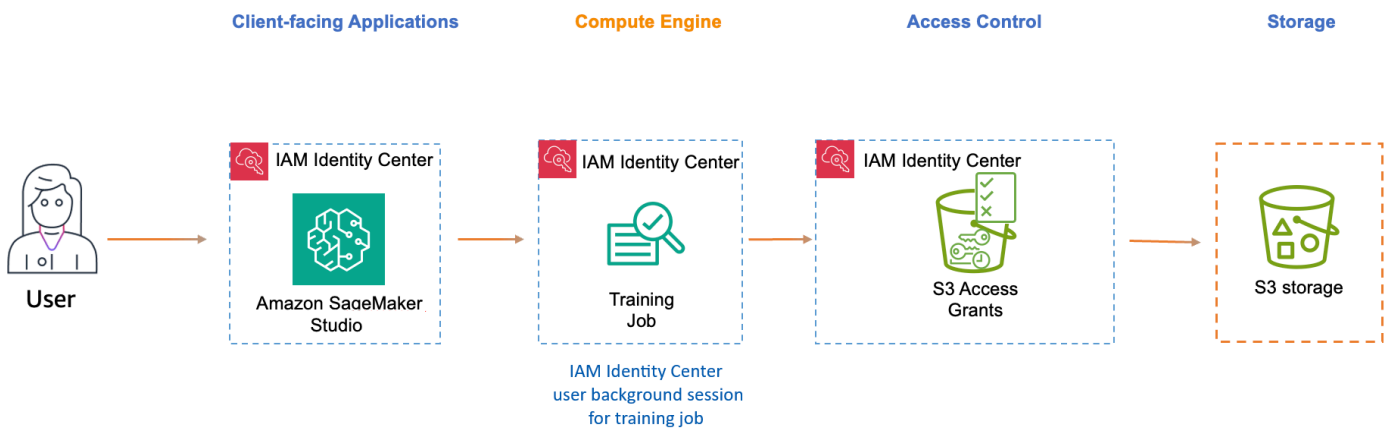
Um die Verbreitung vertrauenswürdiger Identitäten mit Athena einzurichten, muss der Athena-Administrator:

1. Lesen Sie Überlegungen und Einschränkungen bei der Verwendung von IAM Identity Center-fähigen Athena-Arbeitsgruppen.
2. Erstellen Sie eine IAM Identity Center-fähige Athena-Arbeitsgruppe.

Vertrauenswürdige Identitätsverbreitung mit Amazon SageMaker Studio

Amazon SageMaker Studio ist in IAM Identity Center integriert und unterstützt Benutzersitzungen im Hintergrund und die Weitergabe vertrauenswürdiger Identitäten. Benutzerhintergrundsitzungen ermöglichen es einem Benutzer, einen Job mit langer Laufzeit in SageMaker Studio zu initiieren, ohne dass dieser Benutzer angemeldet bleiben muss, während der Job ausgeführt wird. Der Job wird sofort und im Hintergrund ausgeführt, wobei die Berechtigungen des Benutzers verwendet werden, der den Job initiiert hat. Der Job kann auch dann weiter ausgeführt werden, wenn der Benutzer seinen Computer ausschaltet, seine IAM Identity Center-Anmeldesitzung abläuft oder sich der Benutzer vom AWS Access Portal abmeldet. Die Standardsitzungsdauer für Benutzerhintergrundsitzungen beträgt 7 Tage, Sie können jedoch eine maximale Dauer von 90 Tagen angeben. Die Weitergabe vertrauenswürdiger Identitäten ermöglicht einen differenzierten Zugriff auf AWS Ressourcen wie Amazon S3 S3-Buckets auf der Grundlage der Identität oder der Gruppenmitgliedschaft des Benutzers.

Das folgende Diagramm zeigt eine Konfiguration zur Weitergabe vertrauenswürdiger Identitäten für SageMaker Studio mit Zugriff auf Daten, die in einem Amazon S3 S3-Bucket gespeichert sind. Benutzerhintergrundsitzungen sind für IAM Identity Center aktiviert, sodass der SageMaker Studio-Trainingsjob im Hintergrund ausgeführt werden kann. Die Zugriffskontrolle für die Trainingsdaten wird von Amazon S3 bereitgestelltAccess Grants.



AWS verwaltete Anwendung

Die folgende AWS verwaltete Anwendung mit Clientzugriff unterstützt die Weitergabe vertrauenswürdiger Identitäten:

- Amazon SageMaker Studio

Gehen Sie wie folgt vor, um die Verbreitung vertrauenswürdiger Identitäten und Hintergrundsitzungen für Benutzer zu aktivieren:

- Richten Sie SageMaker Studio als Anwendung für den Client ein.
- Richten Sie Amazon S3 einAccess Grants, um den temporären Zugriff auf die zugrunde liegenden Datenspeicherorte in Amazon S3 zu ermöglichen.

Einrichtung der Verbreitung vertrauenswürdiger Identitäten mit SageMaker Studio

Das folgende Verfahren führt Sie durch die Einrichtung von SageMaker Studio für die Verbreitung vertrauenswürdiger Identitäten und Benutzerhintergrundsitzungen.

Voraussetzungen

Bevor Sie mit diesem Tutorial beginnen können, müssen Sie die folgenden Aufgaben erledigen:

1. Aktivieren Sie IAM Identity Center. Eine Organisationsinstanz ist erforderlich. Weitere Informationen finden Sie unter Voraussetzungen und Überlegungen.
2. Stellen Sie die Benutzer und Gruppen aus Ihrer Identitätsquelle im IAM Identity Center bereit.

3. Vergewissern Sie sich, dass Benutzerhintergrundsitzungen in der IAM Identity Center-Konsole aktiviert sind. Standardmäßig sind Benutzerhintergrundsitzungen aktiviert und die Sitzungsdauer ist auf 7 Tage festgelegt. Sie können diese Dauer ändern.

Um die Verbreitung vertrauenswürdiger Identitäten von SageMaker Studio aus einzurichten, muss der SageMaker Studio-Administrator die folgenden Schritte ausführen.

Schritt 1: Aktivieren Sie die Verbreitung vertrauenswürdiger Identitäten in einer neuen oder vorhandenen SageMaker Studio-Domäne

SageMaker Studio verwendet Domänen, um Benutzerprofile, Anwendungen und die zugehörigen Ressourcen zu organisieren. Um die Verbreitung vertrauenswürdiger Identitäten zu aktivieren, müssen Sie eine SageMaker Studio-Domäne erstellen oder eine vorhandene Domäne ändern, wie im folgenden Verfahren beschrieben.

1. Öffnen Sie die SageMaker AI-Konsole, navigieren Sie zu Domains und führen Sie einen der folgenden Schritte aus.

   - Erstellen Sie mithilfe von Setup für Organisationen eine neue SageMaker Studio-Domäne.

     Wählen Sie Für Organisationen einrichten aus, und gehen Sie dann wie folgt vor:

     - Wählen Sie AWS Identity Center als Authentifizierungsmethode.
     - Aktivieren Sie das Kontrollkästchen Weitergabe vertrauenswürdiger Identitäten für alle Benutzer in dieser Domain aktivieren.
   - Ändern Sie eine bestehende SageMaker Studio-Domäne.
     - Wählen Sie eine vorhandene Domäne aus, die IAM Identity Center für die Authentifizierung verwendet.

       Important

       Die Weitergabe vertrauenswürdiger Identitäten wird nur in SageMaker Studio-Domänen unterstützt, die IAM Identity Center zur Authentifizierung verwenden. Wenn die Domäne IAM für die Authentifizierung verwendet, können Sie die Authentifizierungsmethode nicht ändern und daher die Weitergabe vertrauenswürdiger Identitäten nicht aktivieren.

- Bearbeiten Sie die Domäneneinstellungen. Bearbeiten Sie die Authentifizierungs- und Berechtigungseinstellungen, um die Verbreitung vertrauenswürdiger Identitäten zu aktivieren.

2. Fahren Sie mit Schritt 2 fort: Konfigurieren Sie die standardmäßige Ausführungsrolle für die Domäne. Diese Rolle ist erforderlich, damit Benutzer einer SageMaker Studio-Domain auf andere AWS Dienste wie Amazon S3 zugreifen können.

Schritt 2: Konfigurieren Sie die standardmäßige Domänenausführungsrolle und die Rollenvertrauensrichtlinie

Eine Domänenausführungsrolle ist eine IAM-Rolle, die eine SageMaker Studio-Domäne im Namen aller Benutzer in der Domäne übernimmt. Die Berechtigungen, die Sie dieser Rolle zuweisen, bestimmen, welche Aktionen SageMaker Studio ausführen kann.

1. Gehen Sie wie folgt vor, um eine Domain-Ausführungsrolle zu erstellen oder auszuwählen:

   - Erstellen Sie mithilfe von Setup für Organisationen eine Rolle, oder wählen Sie sie aus.
     - Öffnen Sie die SageMaker AI-Konsole und folgen Sie den Anweisungen in Schritt 2: Rollen und ML-Aktivitäten konfigurieren, um eine neue Rolle für die Domain-Ausführung zu erstellen, oder wählen Sie eine vorhandene Rolle aus.
     - Schließen Sie die restlichen Einrichtungsschritte ab, um Ihre SageMaker Studio-Domain zu erstellen.
   - Erstellen Sie manuell eine Ausführungsrolle.
     - Öffnen Sie die IAM-Konsole und erstellen Sie die Ausführungsrolle selbst.

2. Aktualisieren Sie die Vertrauensrichtlinie, die der Domänenausführungsrolle zugeordnet ist, sodass sie die folgenden beiden Aktionen umfasst: `sts:AssumeRole`und `sts:SetContext`. Informationen dazu, wie Sie die Ausführungsrolle für Ihre SageMaker Studio-Domäne finden, finden Sie unter Domänenausführungsrolle abrufen.

   Eine Vertrauensrichtlinie gibt die Identität an, die eine Rolle übernehmen kann. Diese Richtlinie ist erforderlich, damit der SageMaker Studio-Dienst die Rolle der Domänenausführung übernehmen kann. Fügen Sie diese beiden Aktionen hinzu, sodass sie in Ihrer Richtlinie wie folgt angezeigt werden.

```
{

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

```
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "sagemaker.amazonaws.com"
                ]
            },
            "Action": [
                "sts:AssumeRole",
                "sts:SetContext"
            ]
        }
    ]
}
```

Schritt 3: Überprüfen Sie die erforderlichen Amazon S3 Access Grant-Berechtigungen für die Domain-Ausführungsrolle

Um Amazon S3 Access Grants verwenden zu können, müssen Sie Ihrer SageMaker Studio-Domain-Ausführungsrolle eine Berechtigungsrichtlinie (entweder als Inline-Richtlinie oder als vom Kunden verwaltete Richtlinie) angehängt haben, die die folgenden Berechtigungen enthält.

```
{

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

    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetDataAccess",
                "s3:GetAccessGrantsInstanceForPrefix"
                ],
            "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
        }
    ]
}
```

Wenn Sie keine Richtlinie haben, die diese Berechtigungen enthält, folgen Sie den Anweisungen unter Hinzufügen und Entfernen von IAM-Identitätsberechtigungen im AWS Identity and Access Management Benutzerhandbuch.

Schritt 4: Weisen Sie der Domain Gruppen und Benutzer zu

Weisen Sie der SageMaker Studio-Domäne Gruppen und Benutzer zu, indem Sie die Schritte unter Gruppen und Benutzer hinzufügen befolgen.

Schritt 5: Amazon S3 Access Grants einrichten

Um Amazon S3 Access Grants einzurichten, folgen Sie den Schritten unter Konfiguration von Amazon S3 Access Grants für die Weitergabe vertrauenswürdiger Identitäten über das IAM Identity Center. Folgen Sie den step-by-step Anweisungen, um die folgenden Aufgaben zu erledigen:

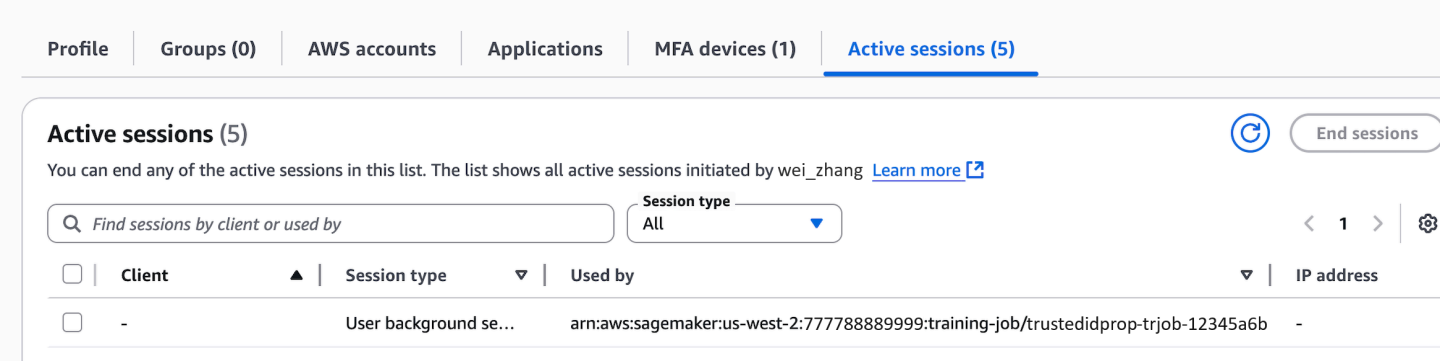
1. Erstellen Sie eine Amazon S3 Access Grants-Instance.
2. Registrieren Sie einen Standort in dieser Instance.
3. Erstellen Sie Zuschüsse, um bestimmten Benutzern oder Gruppen von IAM Identity Center den Zugriff auf bestimmte Amazon S3 S3-Standorte oder Untergruppen (z. B. bestimmte Präfixe) innerhalb dieser Standorte zu ermöglichen.

Schritt 6: Reichen Sie einen SageMaker Schulungsjob ein und sehen Sie sich die Hintergrundinformationen der Benutzer an

Starten Sie in SageMaker Studio ein neues Jupyter-Notizbuch und reichen Sie einen Schulungsjob ein. Führen Sie während der Ausführung des Jobs die folgenden Schritte aus, um die Sitzungsinformationen anzuzeigen und zu überprüfen, ob der Sitzungskontext für den Benutzer im Hintergrund aktiv ist.

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 aktiven Sitzungen für diesen Benutzer an.
5. Um anhand des Amazon-Ressourcennamens (ARN) des Jobs, der die Sitzung verwendet, nach Sitzungen zu suchen, wählen Sie in der Liste Sitzungstyp die Option User background sessions aus und geben Sie dann den Job-ARN in das Suchfeld ein.

Im Folgenden finden Sie ein Beispiel dafür, wie ein Schulungsjob, der eine Benutzer-Hintergrundsitzung verwendet, auf der Registerkarte Aktive Sitzungen für einen Benutzer angezeigt wird.



Schritt 7: Sehen Sie sich die CloudTrail Protokolle an, um die Verbreitung vertrauenswürdiger Identitäten in zu überprüfen CloudTrail

Wenn die Verbreitung vertrauenswürdiger Identitäten aktiviert ist, werden Aktionen in den CloudTrail Ereignisprotokollen unter dem `onBehalfOf` Element angezeigt. Das `userId` gibt die ID des IAM Identity Center-Benutzers wieder, der den Schulungsjob initiiert hat. Das folgende CloudTrail Ereignis erfasst den Prozess der Weitergabe vertrauenswürdiger Identitäten.

```
                        "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA123456789EXAMPLE:SageMaker",
    "arn": "arn:aws:sts::111122223333:assumed-role/SageMaker-
ExecutionRole-20250728T125817/SageMaker",
    "accountId": "111122223333",
    "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
    "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "AROA123456789EXAMPLE",
            "arn": "arn:aws:iam::111122223333:role/service-role/SageMaker-
ExecutionRole-20250728T125817",
            "accountId": "111122223333",
            "userName": "SageMaker-ExecutionRole-20250728T125817"
        },
        "attributes": {
            "creationDate": "2025-07-29T17:17:10Z",
            "mfaAuthenticated": "false"
        }
```

```
    },
    "onBehalfOf": {
        "userId": "2801d3e0-f0e1-707f-54e8-f558b19f0a10",
        "identityStoreArn": "arn:aws:identitystore::777788889999:identitystore/
d-1234567890"
    }
},
```

Überlegungen zur Laufzeit

Wenn ein Administrator MaxRuntimeInSecondsfür lang andauernde Trainings- oder Verarbeitungsaufträge festlegt, die kürzer als die Dauer der Benutzerhintergrundsitzung sind, führt SageMaker Studio den Job mindestens für die Dauer der MaxRuntimeInSeconds Benutzerhintergrundsitzung aus.

Weitere Informationen zu MaxRuntimeInSecondsfinden Sie in der Anleitung für den `CreateTrainingJob` StoppingConditionParameter in der Amazon SageMaker API-Referenz.

Autorisierungsdienste

In allen Analytik- und Data Lakehouse-Anwendungsfällen können Sie mithilfe folgender Methoden detaillierte Zugriffskontrollen erreichen:

- AWS Lake Formation - Eine Anleitung finden Sie unter. Einrichtung AWS Lake Formation mit IAM Identity Center
- Amazon S3 Access Grants — Anleitungen finden Sie unterEinrichtung von Amazon S3 Access Grants mit IAM Identity Center.

Einrichtung AWS Lake Formation mit IAM Identity Center

AWS Lake Formationist ein verwalteter Dienst, der die Erstellung und Verwaltung von Data Lakes auf AWS vereinfacht. Er automatisiert die Datenerfassung, Katalogisierung und Sicherheit und bietet ein zentrales Repository für die Speicherung und Analyse verschiedener Datentypen. Lake Formation bietet detaillierte Zugriffskontrollen und lässt sich in verschiedene AWS Analysedienste integrieren, sodass Unternehmen ihre Data Lakes effizient einrichten, sichern und Erkenntnisse aus ihnen ableiten können.

Gehen Sie wie folgt vor, damit Lake Formation mithilfe von IAM Identity Center und vertrauenswürdiger Identitätsverbreitung Datenberechtigungen auf der Grundlage der Benutzeridentität gewähren kann.

Voraussetzungen

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

- Aktivieren Sie IAM Identity Center. Eine Organisationsinstanz wird empfohlen. Weitere Informationen finden Sie unter Voraussetzungen und Überlegungen.

Schritte zum Einrichten der Verbreitung vertrauenswürdiger Identitäten

1. Integrieren Sie IAM Identity Center und AWS Lake Formation folgen Sie dabei den Anweisungen unter Connecting Lake Formation with IAM Identity Center.

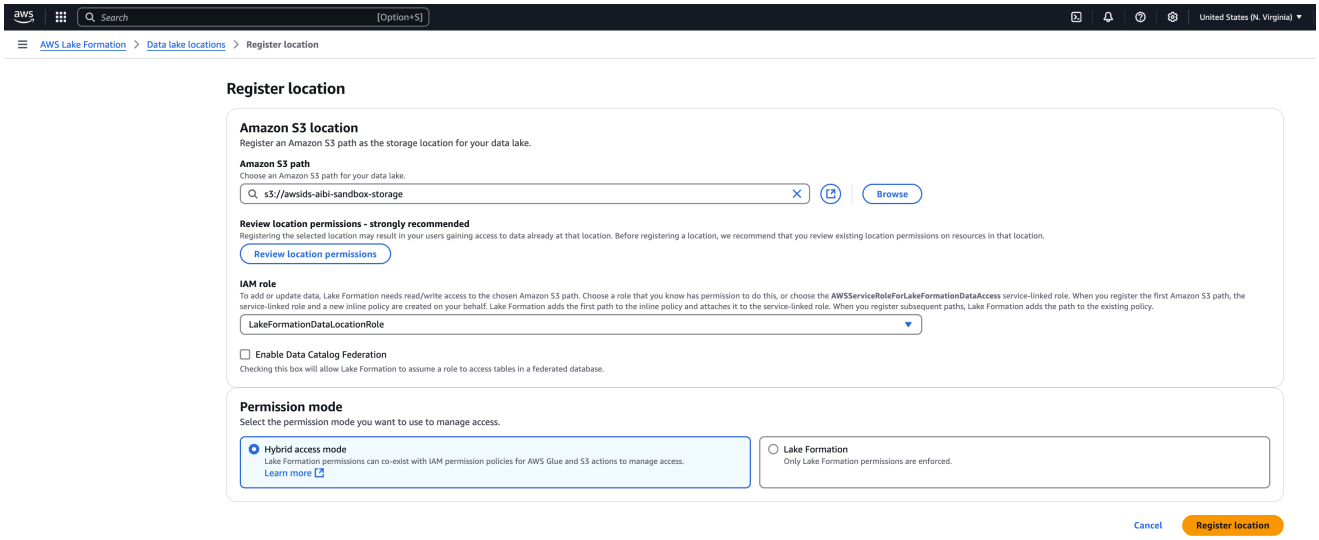
   > **Important**
   >
   > Wenn Sie keine AWS Glue Data Catalog Tabellen haben, müssen Sie diese erstellen, um IAM Identity Center-Benutzern und -Gruppen Zugriff gewähren zu können AWS Lake Formation . Weitere Informationen finden Sie unter Objekte erstellen in AWS Glue Data Catalog.

2. Registrieren Sie Data Lake-Standorte.

   Registrieren Sie die S3-Standorte, an denen die Daten der Glue-Tabellen gespeichert sind. Auf diese Weise gewährt Lake Formation temporären Zugriff auf die erforderlichen S3-Speicherorte, wenn die Tabellen abgefragt werden, sodass keine S3-Berechtigungen in die Servicerolle aufgenommen werden müssen (z. B. die auf dem konfigurierte Athena-Servicerolle). WorkGroup

   a. Navigieren Sie im Navigationsbereich der Konsole im Bereich Administration zu den Data Lake-Speicherorten. AWS Lake Formation Wählen Sie Standort registrieren aus.

      Auf diese Weise kann Lake Formation temporäre IAM-Anmeldeinformationen mit den erforderlichen Berechtigungen für den Zugriff auf S3-Datenstandorte bereitstellen.



b. Geben Sie den S3-Pfad der Datenspeicherorte der AWS Glue Tabellen in das Feld Amazon S3 S3-Pfad ein.

c. Wählen Sie im Abschnitt „IAM-Rolle“ nicht die mit dem Service verknüpfte Rolle aus, wenn Sie sie mit der Verbreitung vertrauenswürdiger Identitäten verwenden möchten. Erstellen Sie eine separate Rolle mit den folgenden Berechtigungen.

   Um diese Richtlinien zu verwenden, ersetzen Sie die Richtlinie *`italicized placeholder text`* im Beispiel durch Ihre eigenen Informationen. Weitere Anweisungen finden Sie unter Richtlinie erstellen oder Richtlinie bearbeiten. Die Berechtigungsrichtlinie sollte Zugriff auf den S3-Standort gewähren, der im folgenden Pfad angegeben ist:

   i. Genehmigungsrichtlinie:

      JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "LakeFormationDataAccessPermissionsForS3",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject"
```

```
            ],
            "Resource": [
                "arn:aws:s3:::Your-S3-Bucket/*"
            ]
        },
        {
            "Sid":
 "LakeFormationDataAccessPermissionsForS3ListBucket",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::Your-S3-Bucket"
            ]
        },
        {
            "Sid": "LakeFormationDataAccessServiceRolePolicy",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": [
                "arn:aws:s3:::*"
            ]
        }
    ]
}
```

ii. Vertrauensverhältnis: Dies sollte Folgendes beinhalten`sts:SectContext`, was für die Weitergabe vertrauenswürdiger Identitäten erforderlich ist.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "lakeformation.amazonaws.com"
            },
```

```
            "Action": [
                "sts:AssumeRole",
                "sts:SetContext"
            ]
        }
    ]
}
```

> **Note**
>
> Die vom Assistenten erstellte IAM-Rolle ist eine dienstbezogene Rolle und umfasst nicht. `sts:SetContext`

d. Wählen Sie nach dem Erstellen der IAM-Rolle die Option Standort registrieren aus.

Vertrauenswürdige Identitätsverbreitung mit Lake Formation auf AWS-Konten

AWS Lake Formation unterstützt die gemeinsame Nutzung von AWS Resource Access Manager (RAM) für die gemeinsame Nutzung von Tabellen AWS-Konten und funktioniert mit der Weitergabe vertrauenswürdiger Identitäten, wenn sich das Grantor-Konto und das Empfängerkonto in derselben AWS-Region, in derselben AWS Organizations Organisationsinstanz von IAM Identity Center befinden und dieselbe Organisationsinstanz verwenden. Weitere Informationen finden Sie unter Kontoübergreifender Datenaustausch in Lake Formation.

Einrichtung von Amazon S3 Access Grants mit IAM Identity Center

Amazon S3 Access Grants bietet die Flexibilität, eine identitätsbasierte, detaillierte Zugriffskontrolle für S3-Standorte zu gewähren. Sie können Amazon S3 verwendenAccess Grants, um Ihren Unternehmensbenutzern und -gruppen direkten Zugriff auf den Amazon S3 S3-Bucket zu gewähren. Folgen Sie diesen Schritten, um S3 Access Grants mit IAM Identity Center zu aktivieren und eine vertrauenswürdige Identitätsverbreitung zu erreichen.

Voraussetzungen

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

- Aktivieren Sie IAM Identity Center. Eine Organisationsinstanz wird empfohlen. Weitere Informationen finden Sie unter Voraussetzungen und Überlegungen.

Konfiguration von S3 Access Grants für die Verbreitung vertrauenswürdiger Identitäten über das IAM Identity Center

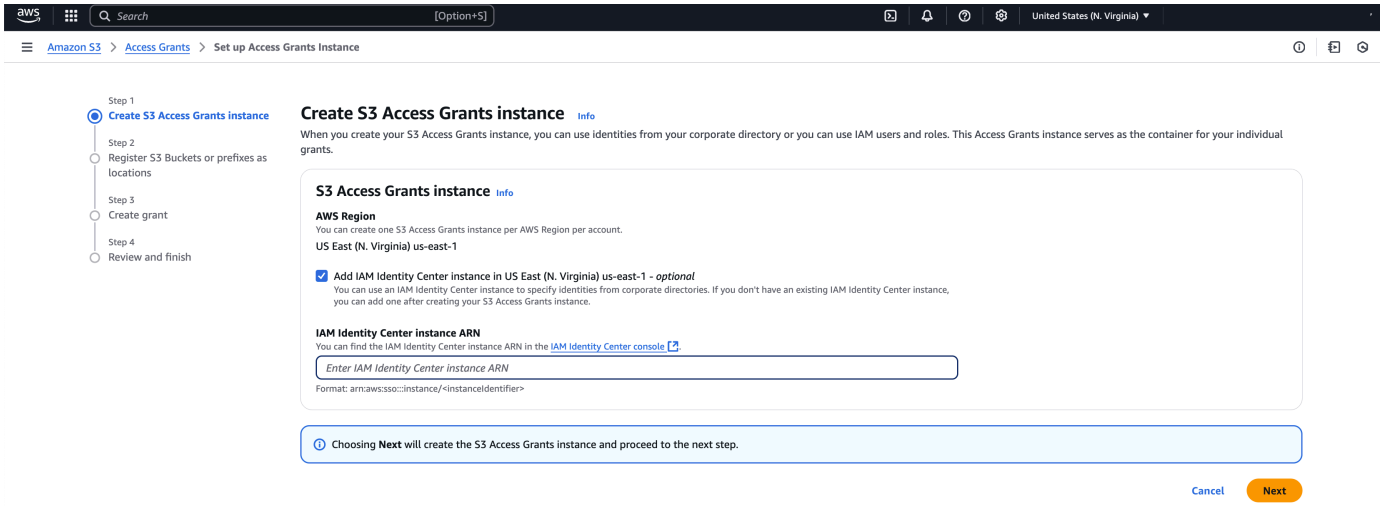
Wenn Sie bereits eine Amazon S3 Access Grants S3-Instance mit einem registrierten Standort haben, gehen Sie wie folgt vor:

1. Ordnen Sie Ihre IAM Identity Center-Instance zu.
2. Erstellen Sie einen Zuschuss.

Wenn Sie noch kein Amazon S3 Access Grants erstellt haben, gehen Sie wie folgt vor:

1. Eine Access Grants S3-Instance erstellen — Sie können jeweils eine Access Grants S3-Instance erstellen AWS-Region. Achten Sie beim Erstellen der Access Grants S3-Instanz darauf, das Kästchen IAM Identity Center-Instanz hinzufügen zu aktivieren und den ARN Ihrer IAM Identity Center-Instanz anzugeben. Klicken Sie auf Weiter.

   Die folgende Abbildung zeigt die Seite „Access GrantsS3-Instance erstellen“ in der Amazon S3 Access Grants S3-Konsole:



2. Standort registrieren — Nachdem Sie eine Amazon S3 Access Grants S3-Instance AWS-Region in Ihrem Konto erstellt und erstellt haben, registrieren Sie einen S3-Standort in dieser Instance. Ein Access Grants S3-Standort ordnet die Standard-S3-Region (`s3://`), einen Bucket oder ein Präfix einer IAM-Rolle zu. S3 Access Grants übernimmt diese Amazon S3 S3-Rolle, um temporäre Anmeldeinformationen an den Empfänger weiterzugeben, der auf diesen bestimmten

Standort zugreift. Sie müssen zuerst mindestens einen Standort in Ihrer Access Grants S3-Instance registrieren, bevor Sie eine Zugriffsberechtigung erstellen können.

Geben Sie für den Bereich Standort an`s3://`, der alle Ihre Buckets in dieser Region umfasst. Dies ist der empfohlene Standortbereich für die meisten Anwendungsfälle. Wenn Sie ein Anwendungsbeispiel für erweitertes Zugriffsmanagement haben, können Sie den Standortbereich auf einen bestimmten Bereich `s3://`*`bucket`* oder ein bestimmtes Präfix innerhalb eines Buckets festlegen`s3://`*`bucket`*`/`*`prefix-with-path`*. Weitere Informationen finden Sie unter Einen Standort registrieren im Amazon Simple Storage Service-Benutzerhandbuch.

> **Note**
>
> Stellen Sie sicher, dass die S3-Speicherorte der AWS Glue Tabellen, auf die Sie Zugriff gewähren möchten, in diesem Pfad enthalten sind.

Das Verfahren erfordert, dass Sie eine IAM-Rolle für den Standort konfigurieren. Diese Rolle sollte Berechtigungen für den Zugriff auf den Standortbereich beinhalten. Sie können den S3-Konsolenassistenten verwenden, um die Rolle zu erstellen. Sie müssen Ihren Access Grants S3-Instance-ARN in den Richtlinien für diese IAM-Rolle angeben. Der Standardwert Ihres Access Grants S3-Instance-ARN ist`arn:aws:s3:`*`Your-Region`*`:`*`Your-AWS-Account-ID`*`:access-grants/default`.

Die folgende Beispielberechtigungsrichtlinie erteilt Amazon S3 S3-Berechtigungen für die von Ihnen erstellte IAM-Rolle. Und die darauf folgende Beispiel-Vertrauensrichtlinie ermöglicht es dem Access Grants S3-Serviceprinzipal, die IAM-Rolle zu übernehmen.

a. Berechtigungsrichtlinie

   Um diese Richtlinien zu verwenden, ersetzen Sie die Richtlinie *`italicized placeholder text`* im Beispiel durch Ihre eigenen Informationen. Weitere Anweisungen finden Sie unter Richtlinie erstellen oder Richtlinie bearbeiten.

   JSON

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

```
    "Statement": [
        {
            "Sid": "ObjectLevelReadPermissions",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion",
                "s3:GetObjectAcl",
                "s3:GetObjectVersionAcl",
                "s3:ListMultipartUploadParts"
            ],
            "Resource": [
                "arn:aws:s3:::*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "111122223333"
                },
                "ArnEquals": {
                    "s3:AccessGrantsInstanceArn": [
                    "arn:aws:s3:::access-grants/instance-id"
                    ]
                }
            }
        },
        {
            "Sid": "ObjectLevelWritePermissions",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectVersionAcl",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:AbortMultipartUpload"
            ],
            "Resource": [
                "arn:aws:s3:::*"
            ],
            "Condition": {
                "StringEquals": {
                "aws:ResourceAccount": "111122223333"
                },
                "ArnEquals": {
```

```
                    "s3:AccessGrantsInstanceArn": [
                    "arn:aws:s3:::access-grants/instance-id"
                    ]
                }
            }
        },
        {
            "Sid": "BucketLevelReadPermissions",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::*"
            ],
            "Condition": {
                "StringEquals": {
                "aws:ResourceAccount": "111122223333"
                },
                "ArnEquals": {
                    "s3:AccessGrantsInstanceArn": [
                    "arn:aws:s3:::access-grants/instance-id"
                    ]
                }
            }
        },
        {
            "Sid": "OptionalKMSPermissionsForSSEEncryption",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

b. Vertrauensrichtlinie

Gewähren Sie in der Vertrauensrichtlinie für IAM-Rollen dem S3-Access-Grants-Service (`access-grants.s3.amazonaws.com`)-Prinzipal Zugriff auf die IAM-Rolle, die Sie erstellt

haben. Hierzu können Sie eine JSON-Datei mit den folgenden Anweisungen erstellen. Informationen zum Hinzufügen der Vertrauensrichtlinie zu Ihrem Konto finden Sie unter Erstellen einer Rolle mit benutzerdefinierten Vertrauensrichtlinien.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1234567891011",
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole",
                "sts:SetSourceIdentity"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333",
                    "aws:SourceArn": "Your-Custom-Access-Grants-Location-
ARN"
                }
            }
        },

        {
            "Sid": "Stmt1234567891012",
            "Effect": "Allow",
            "Action": "sts:SetContext",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333",
                    "aws:SourceArn": "Your-Custom-Access-Grants-Location-
ARN"
                },
                "ForAllValues:ArnEquals": {
                    "sts:RequestContextProviders":
 "arn:aws:iam::aws:contextProvider/IdentityCenter"
                }
            }
```

```
        }
    ]
}
```

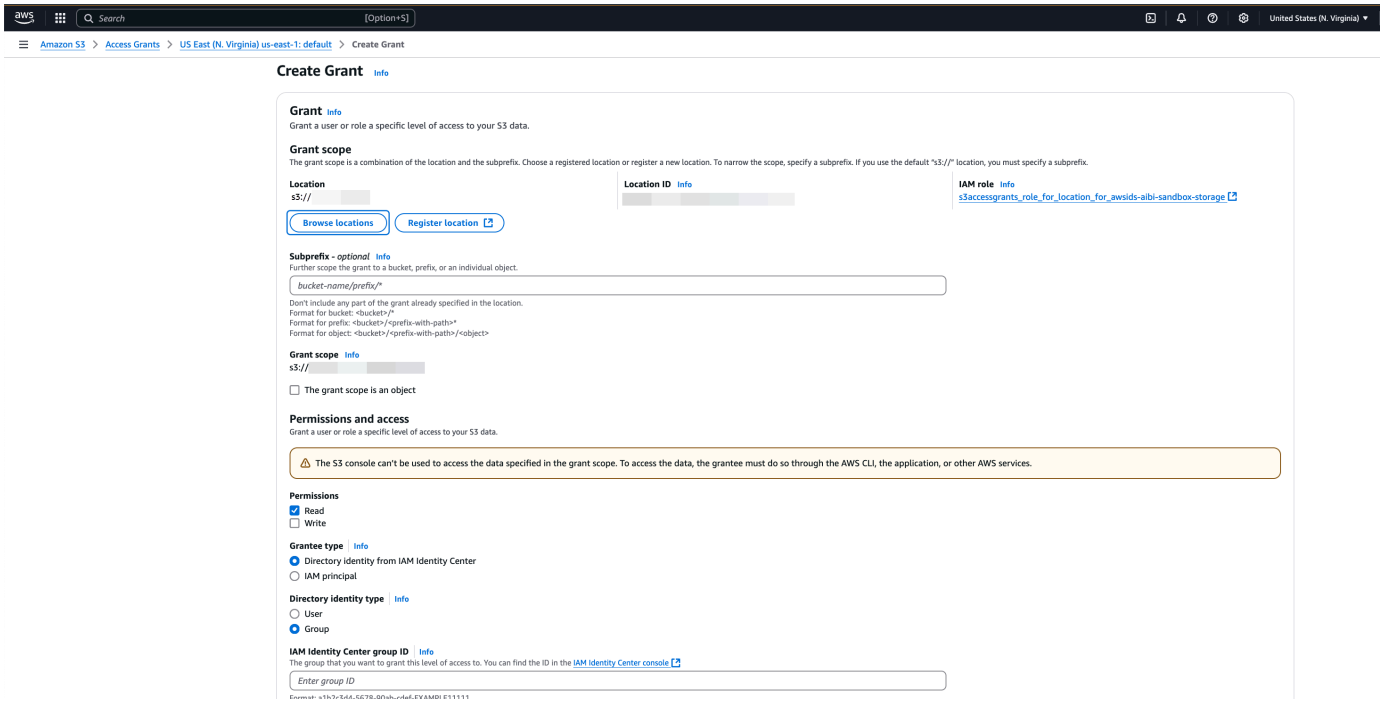
Amazon S3 Access Grant erstellen

Wenn Sie über eine Amazon S3 Access Grants S3-Instance mit einem registrierten Standort verfügen und Ihre IAM Identity Center-Instance damit verknüpft haben, können Sie einen Grant erstellen. Gehen Sie auf der Seite „Grant erstellen“ der S3-Konsole wie folgt vor:

Erstellen einer Erteilung

1. Wählen Sie den im vorherigen Schritt erstellten Standort aus. Sie können den Umfang des Zuschusses reduzieren, indem Sie ein Unterpräfix hinzufügen. Das Unterpräfix kann ein `bucketbucket/prefix`, oder ein Objekt im Bucket sein. Weitere Informationen finden Sie unter Subprefix im Amazon Simple Storage Service-Benutzerhandbuch.
2. Wählen Sie unter Berechtigungen und Zugriff je nach Bedarf Lesen und/oder Schreiben aus.
3. Wählen Sie unter Granter type die Option Directory Identity form IAM Identity Center aus.
4. Geben Sie die IAM Identity Center-Benutzer- oder Gruppen-ID ein. Sie finden den Benutzer und die Gruppe IDs in der IAM Identity Center-Konsole in den Abschnitten Benutzer und Gruppe. Klicken Sie auf Weiter.
5. Überprüfen Sie auf der Seite „Überprüfen und beenden“ die Einstellungen für den S3 Access Grant und wählen Sie dann Create Grant aus.

   Die folgende Abbildung zeigt die Seite „Grant erstellen“ in der Amazon S3 Access Grants S3-Konsole:



Richten Sie Ihre eigene OAuth 2.0-Anwendung ein

Die Verbreitung vertrauenswürdiger Identitäten ermöglicht es einer vom Kunden verwalteten Anwendung, im Namen eines Benutzers Zugriff auf Daten in AWS Diensten anzufordern. 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 weitergeben. AWS-Services

> **Important**
>
> Um auf eine vom Kunden verwaltete Anwendungen zugreifen zu können AWS-Service, müssen sie 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 Zugriffsanfragen auf AWS-Services (Empfangen von Anwendungen)

initiieren. 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

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 aus

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie Applications (Anwendungen).
3. Wählen Sie die Registerkarte Vom Kunden verwaltet aus.
4. Wählen Sie Anwendung hinzufügen.
5. Wählen Sie auf der Seite Anwendungstyp auswählen unter Einrichtungspräferenz 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 gelangenSchritt 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, vorausgesetzt, dass 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 oder nicht sichtbar sein soll. 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 Ressourcen taggen AWS IAM Identity Center.
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 (Anträge anfordern) 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-Aussteller 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 Enable refresh token grant aus. 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 `CreateTokenWithIAM`API-Aktion. Weitere Informationen zu dieser Richtlinie und ein Beispiel, das Sie nach Bedarf an Ihre Umgebung anpassen können, finden Sie unterBeispiel für eine ressourcenbasierte Richtlinie für IAM Identity Center (IAM Identity Center).

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 unter Kontoübergreifender Zugriff mithilfe ressourcenbasierter Richtlinien und IAM ARNs im Benutzerhandbuch.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 eine oder mehrere AWS-Services 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 aus.
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 Verbreitung von Identitäten die Option Vertrauenswürdige Anwendungen angeben aus.
6. Wählen Sie unter Setuptyp 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 aus, 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 Anzuwendende Zugriffsebene die Zugriffsebenen nach Bedarf und wählen Sie dann Änderungen speichern aus.

- Dieselbe Zugriffsebene auf alle Anwendungen anwenden — Wählen Sie diese Option, wenn Sie die Zugriffsebenen nicht für jede 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.

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 für den Zugriff auf (Empfangen von Anwendungen) initiieren AWS-

Services(Anwendungen anfordern). 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-Services Benutzer, die Anfragen erhalten, verwalten eine detaillierte Autorisierung für ihre Ressourcen auf der Grundlage ihrer Benutzer und Gruppenzugehörigkeit, wie sie im Identity Center-Verzeichnis dargestellt sind. AWS-Services kann die Token des externen Token-Emittenten 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. Der vertrauenswürdige Token-Aussteller ist zwar in der Regel der Identitätsanbieter, den Sie als Identitätsquelle für IAM Identity Center verwenden, muss es aber nicht 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 und im Format JSON Web Token (JWT) sein, wobei der Algorithmus verwendet wird RS256.
  - 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. Auf diesen wird zugegriffen AWS-Service , nachdem das Token gegen ein Token von IAM Identity Center eingetauscht 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.

> **Note**
>
> Die Verwendung eines benutzerdefinierten Signaturschlüssels für JWTs from Microsoft Entra ID wird nicht unterstützt. Um Token von Microsoft Entra ID einem vertrauenswürdigen Token-Aussteller zu verwenden, können Sie keinen benutzerdefinierten Signaturschlüssel verwenden.

- 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-Antrag

- 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.

Einzelheiten zum JTI-Antrag

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 Tokens, 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 keinen 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.
> Die URL des OIDC-Discovery-Endpunkts darf nur über die Ports 80 und 443 erreichbar sein.

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-Aussteller 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-Aussteller 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-Identitätsspeicherattribute 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 (an AWS-Service) zu stellen.

Themen

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. Benachrichtigt den AWS Dienstadministrator, wenn der vertrauenswürdige Token-Aussteller der IAM Identity Center-Konsole hinzugefügt wird.	Externer IdP-Administrator (vertrauenswürdiger Token-Aussteller) AWS Dienstadministrator
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.	IAM Identity Center-Administrator Externer IdP-Administrator (vertrauenswürdiger Token-Aussteller)

Rolle	Führt diese Aufgaben aus	Koordiniert mit
	Konfiguriert den AWS Dienst für die Verwendung des vertrauen swürdigen Token-Ausstellers.	

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 hinzu oder. APIs 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). Der Discovery-Endpunkt darf nur über die Ports 80 und 443 erreichbar sein.
   - 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 Dienst mit dem IAM Identity Center verbinden — Der AWS Dienstadministrator muss die Anwendung mit dem IAM Identity Center verbinden, indem er die Konsole für die Anwendung oder die Anwendung verwendet. APIs

   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-Claim-Wert 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 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 Ressourcen taggen AWS IAM Identity Center.

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.

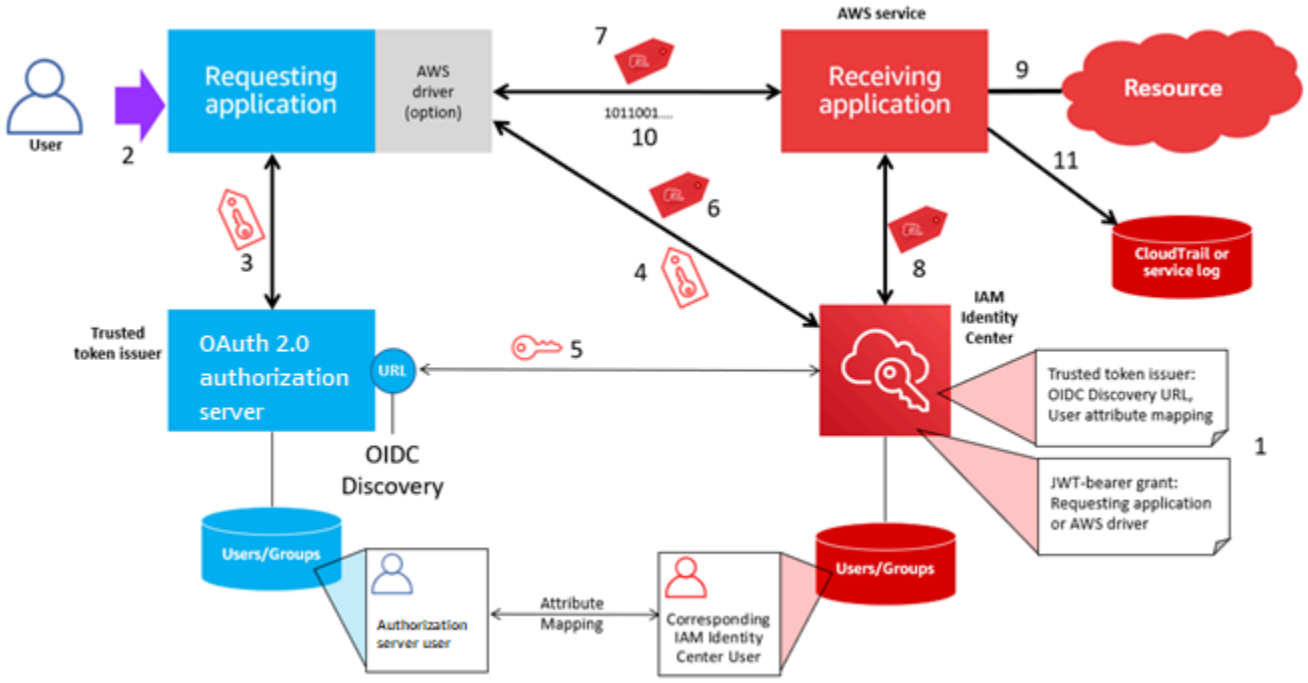
Wenn Sie beabsichtigen, die Einstellungen des vertrauenswürdigen Token-Ausstellers zu bearbeiten, denken Sie daran, dass Benutzer dadurch den Zugriff auf alle Anwendungen verlieren können, die für die Verwendung des vertrauenswürdigen Token-Ausstellers konfiguriert sind. Um eine Unterbrechung des Benutzerzugriffs 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 Einstellungen aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Authentifizierung aus.
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 werden in den Protokollen und CloudTrail Ereignissen der empfangenden Anwendung aufgezeichnet. Die spezifische Art und Weise, wie diese Informationen protokolliert werden, ist je nach Anwendung unterschiedlich.

IAM-Rollensitzungen mit verbesserter Identität

Das AWS Security Token Service(STS) ermöglicht es einer Anwendung, eine identitätserweiterte IAM-Rollensitzung abzurufen. Rollensitzungen mit erweiterter Identität verfügen über einen zusätzlichen Identitätskontext, der dem aufgerufenen eine Benutzerkennung beifügt. AWS-Service AWS-Services kann die Gruppenmitgliedschaften und Attribute des Benutzers in IAM Identity Center nachschlagen und sie verwenden, um den Zugriff des Benutzers auf Ressourcen zu autorisieren.

AWS Anwendungen rufen Rollensitzungen mit erweiterter Identität ab, indem sie Anfragen an die AWS STS AssumeRoleAPI-Aktion stellen und eine Kontext-Assertion mit der Benutzerkennung (`userId`) im Parameter der `ProvidedContexts` Anfrage an übergeben. `AssumeRole` Die Kontext-Assertion wird aus dem `idToken` Anspruch abgerufen, der als Antwort auf eine Anfrage an eingegangen ist. `SSO OIDC` `CreateTokenWithIAM` Wenn eine AWS Anwendung eine Rollensitzung mit erweiterter Identität für den Zugriff auf eine Ressource verwendet, werden die `userId` initiierende Sitzung und die ausgeführte Aktion CloudTrail protokolliert. Weitere Informationen finden Sie unter Protokollierung von IAM-Rollensitzungen mit verbesserter Identität.

Themen

- Arten von IAM-Rollensitzungen mit erweiterter Identität
- Protokollierung von IAM-Rollensitzungen mit verbesserter Identität

Arten von IAM-Rollensitzungen mit erweiterter Identität

AWS STS kann zwei verschiedene Typen von IAM-Rollensitzungen mit verbesserter Identität erstellen, je nachdem, welche Kontext-Assertion für die Anfrage angegeben wurde. `AssumeRole` Anwendungen, die ID-Token von IAM Identity Center erhalten haben, können IAM-Rollensitzungen hinzufügen `sts:identiy_context` (empfohlen) oder `sts:audit_context` (aus Gründen der Abwärtskompatibilität unterstützt). Eine IAM-Rollensitzung mit erweiterter Identität kann nur eine dieser Kontext-Assertionen haben, nicht beide.

IAM-Rollensitzungen mit verbesserter Identität, erstellt mit **`sts:identity_context`**

Wenn eine Rollensitzung mit erweiterter Identität `sts:identity_context` die aufgerufenen enthält, wird AWS-Service bestimmt, ob die Ressourcenautorisierung auf dem Benutzer basiert, der in der Rollensitzung vertreten ist, oder ob sie auf der Rolle basiert. AWS-Services Diese unterstützen die benutzerbasierte Autorisierung und bieten dem Administrator der Anwendung die Möglichkeit, dem Benutzer oder Gruppen, denen der Benutzer angehört, Zugriff zuzuweisen.

AWS-Services die keine benutzerbasierte Autorisierung unterstützen, ignorieren die. `sts:identity_context` CloudTrail protokolliert die userId des IAM Identity Center-Benutzers mit allen von der Rolle ausgeführten Aktionen. Weitere Informationen finden Sie unter Protokollierung von IAM-Rollensitzungen mit verbesserter Identität.

Um diese Art von Rollensitzung mit erweiterter Identität abzurufen AWS STS, stellen Anwendungen den Wert des `sts:identity_context` Felds in der AssumeRoleAnfrage mithilfe des Anforderungsparameters bereit. `ProvidedContexts` Verwenden Sie `arn:aws:iam::aws:contextProvider/IdentityCenter` ihn als Wert für. `ProviderArn`

Weitere Informationen zum Verhalten der Autorisierung finden Sie in der Dokumentation zum Empfang AWS-Service.

IAM-Rollensitzungen mit verbesserter Identität, erstellt mit **`sts:audit_context`**

In der Vergangenheit `sts:audit_context` wurde es verwendet, um die Benutzeridentität AWS-Services zu protokollieren, ohne sie für eine Autorisierungsentscheidung zu verwenden. AWS-Services sind nun in der Lage, einen einzigen Kontext zu `sts:identity_context` verwenden, um dies zu erreichen und Autorisierungsentscheidungen zu treffen. Wir empfehlen die Verwendung von Trusted Identity Propagation `sts:identity_context` in allen neuen Bereitstellungen.

Protokollierung von IAM-Rollensitzungen mit verbesserter Identität

Wenn eine Anfrage an eine Sitzung gestellt wird, die eine identitätserweiterte IAM-Rollensitzung AWS-Service verwendet, wird das IAM Identity Center `userId` des Benutzers im Element angemeldet. CloudTrail `onBehalfOf` Die Art und Weise, wie Ereignisse angemeldet werden, CloudTrail hängt vom ab. AWS-Service Nicht alle AWS-Services protokollieren das `onBehalfOf` Element.

Im Folgenden finden Sie ein Beispiel dafür, wie eine Anfrage, die an eine Sitzung gestellt wurde, bei der eine Rolle AWS-Service mit erweiterter Identität verwendet wird, angemeldet wird. CloudTrail

```
"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"
    }
}
```

Wechseln Sie die IAM Identity Center-Zertifikate

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.

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 die Vertrauensstellung 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 aus.

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

In der IAM Identity Center-Konsole werden auf der Anwendungsseite Statusanzeigesymbole in den Eigenschaften der einzelnen Anwendungen angezeigt. 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 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 Anträge den Status der Zertifikate in der Liste, wie in der Spalte Läuft ab am angegeben.

Machen Sie sich mit den Anwendungseigenschaften in der IAM Identity Center-Konsole vertraut

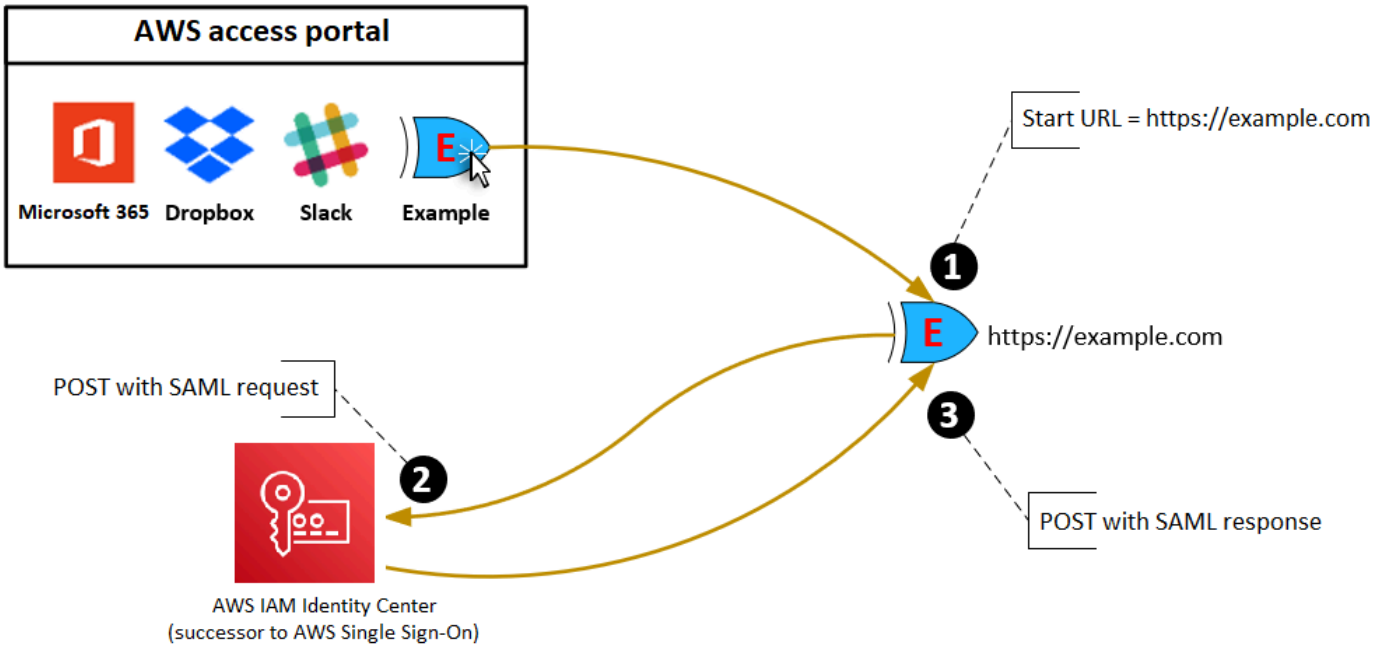
In IAM Identity Center können Sie die Benutzererfahrung anpassen, indem Sie die Start-URL der Anwendung, den Relay-Status und die Sitzungsdauer konfigurieren.

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.

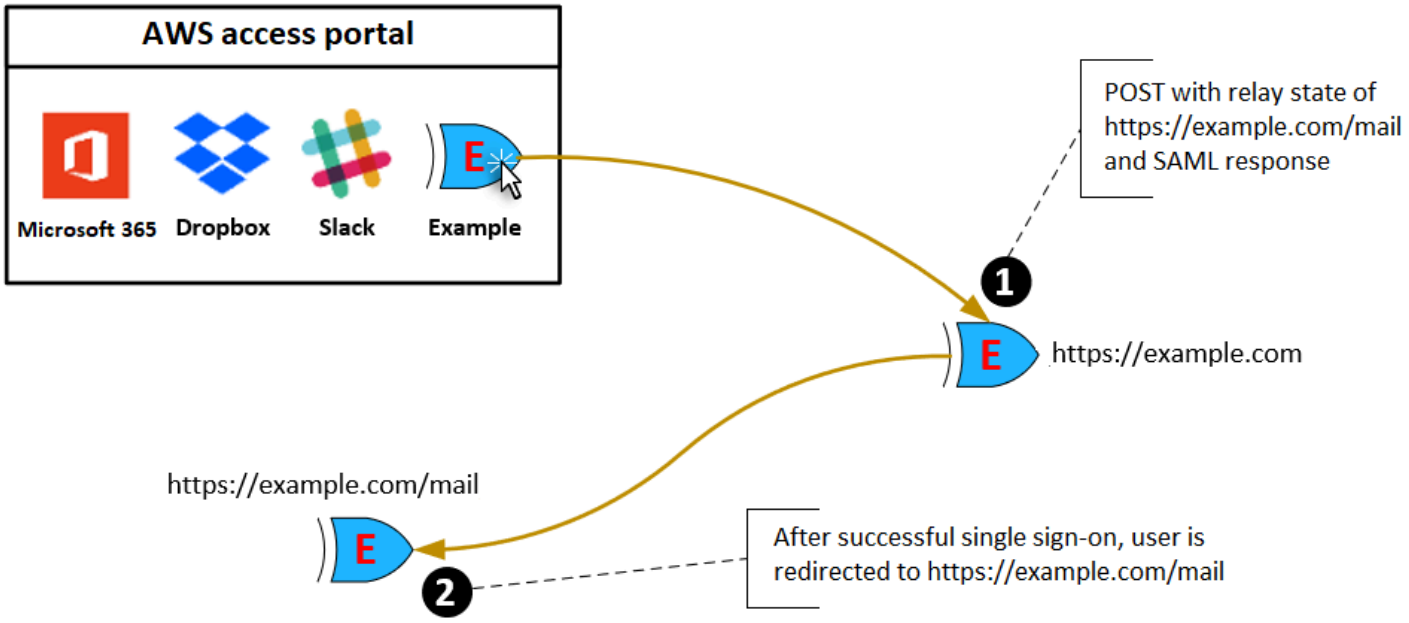
Die folgenden Schritte und das Diagramm veranschaulichen den Ablauf der URL-Authentifizierung beim Starten einer Anwendung, wenn ein Benutzer im AWS Access Portal eine Anwendung auswählt:

1. Der Browser des Benutzers leitet die Authentifizierungsanfrage mithilfe des Werts für die Start-URL der Anwendung weiter (in diesem Fall https://example.com).
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**
>
> Für AWS verwaltete Anwendungen müssen Sie Benutzer direkt aus den entsprechenden Anwendungskonsolen oder über die hinzufügen APIs.

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 Benutzeranzeigenamen oder einen Gruppennamen ein. Sie können mehrere Benutzer oder Gruppen angeben, indem Sie die entsprechenden Konten auswählen, so wie sie in den Suchergebnissen angezeigt werden.
6. Wählen Sie Assign users (Benutzer zuweisen) aus.

Entfernen Sie den Benutzerzugriff auf SAML 2.0-Anwendungen

Gehen Sie wie folgt vor, um den Benutzerzugriff auf SAML 2.0-Anwendungen im Anwendungskatalog oder auf benutzerdefinierte SAML 2.0-Anwendungen zu entfernen. Weitere Informationen zu Authentifizierungssitzungen und deren Dauer finden Sie unter. Grundlegendes zu Authentifizierungssitzungen in IAM Identity Center

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 zwischen dem IAM Identity Center und dem Verzeichnis externer Identitätsanbieter
8. Wählen Sie in der dritten Spalte der Tabelle das entsprechende Format für das Attribut aus dem Menü aus.
9. Wählen Sie Änderungen speichern aus.

Konfigurieren Sie den Zugriff auf AWS-Konten

AWS IAM Identity Center ist in integriert AWS Organizations, sodass Sie Berechtigungen für mehrere Konten 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 AWS-Konten mithilfe einer Organisationsinstanz von IAM Identity Center zu kontrollieren. Kontoinstanzen von IAM Identity Center unterstützen keinen Kontozugriff.

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
Vom Kunden verwaltete Anwendungen erstellen, bearbeiten oder löschen	Nein	Ja	Ja
AWS Verwaltete Anwendungen erstellen, bearbeiten oder löschen	Ja	Ja	Ja

Verwaltungsaufgaben von IAM Identity Center	Mitgliedskonto	Delegiertes Administratorkonto	Verwaltungskonto
MFA konfigurieren	 Nein	 Ja	 Ja
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

Verwaltungsaufgaben von IAM Identity Center	Mitgliedskonto	Delegiertes Administratorkonto	Verwaltungskonto
Registrieren oder deregistrieren Sie ein Mitgliedskonto als delegierter Administrator	 Nein	 Nein	 Ja

*Informationen zu Benutzer- und Gruppenzuweisungen zum Verwaltungskonto finden Sie in den bewährten Methoden für die delegierte Administration.

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 Konfigurieren Sie den Zugriff auf Anwendungen.

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-Managementkonsole, 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-Managementkonsole oder temporäre Anmeldeinformationen abrufen, um programmgesteuert auf AWS Dienste zuzugreifen.

Um die temporären Anmeldeinformationen für den AWS programmgesteuerten Zugriff zu öffnen AWS-Managementkonsole 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-Managementkonsole.
6. Zusätzlich zur Rolle können AWS Access-Portal-Benutzer temporäre Anmeldeinformationen für den Befehlszeilen- oder programmgesteuerten Zugriff abrufen, indem sie Zugriffstasten wählen.

step-by-stepAnleitungen, die Sie Ihren Mitarbeitern zur Verfügung stellen können, finden Sie unter Einrichtung und Nutzung des AWS Zugangsportals undAbrufen der IAM Identity Center-Benutzeranmeldedaten für oder AWS CLIAWS SDKs.

Erzwingung und Beschränkung des Zugriffs

Wenn Sie IAM Identity Center aktivieren, erstellt IAM Identity Center eine dienstbezogene Rolle. Sie können auch Richtlinien zur Dienststeuerung () verwenden. SCPs

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 erhalten Sie unter Grundlegendes zu serviceverknüpften Rollen in IAM Identity Center 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**
>
> Um sicherzustellen, dass Ihre AWS verwalteten Anwendungen gut mit Ihrem IAM Identity Center funktionieren, sollten Sie es vermeiden, dieses SCP dort anzuwenden, AWS-Konten wo Sie diese Anwendungen bereitgestellt haben. Wenn Sie die delegierte Administration verwenden, sollten Sie außerdem vermeiden, diesen SCP auf das Konto für die delegierte Administration anzuwenden. Weitere Informationen finden Sie unter Bewährte Methoden.

Weitere Informationen finden Sie unter Richtlinien zur Dienststeuerung (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 unterKonfigurieren Sie den Zugriff 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 um das Prinzip der geringsten Rechte einzuhalten, 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. Sie können auch erwägen, temporären erweiterten Zugriff zu verwenden, um diesen Zugriff nur bei Bedarf zu gewähren.
- Dedizierte Berechtigungssätze für das Verwaltungskonto — Verwenden Sie spezielle Berechtigungssätze für das Verwaltungskonto. Aus Sicherheitsgründen kann ein für den Zugriff auf das Verwaltungskonto verwendeter Berechtigungssatz nur von einem IAM Identity Center-Administrator über das Verwaltungskonto geändert werden. Der delegierte Administrator kann die im Verwaltungskonto bereitgestellten Berechtigungssätze nicht ändern.
- Zuweisen von Benutzern (nicht Gruppen) zu Berechtigungssätzen im Verwaltungskonto — Da das Verwaltungskonto über besondere Rechte verfügt, müssen Sie bei der Zuweisung von Zugriff auf dieses Konto in der Konsole oder AWS Command Line Interface (CLI) Vorsicht walten lassen. Wenn Sie Gruppen Berechtigungssätzen mit Zugriff auf das Verwaltungskonto zuweisen, kann jeder, der berechtigt ist, die Mitgliedschaften in diesen Gruppen zu ändern, add/remove to/from diese Gruppen verwenden und somit beeinflussen, wer Zugriff auf das Verwaltungskonto hat. Dies ist ein beliebiger Gruppenadministrator mit Kontrolle über Ihre Identitätsquelle, einschließlich Ihres Identitätsanbieters (IdP) -Administrators, Microsoft Active Directory Domain Service (AD DS) -Administrators oder IAM Identity Center-Administrators. Daher sollten Sie Benutzer direkt Berechtigungssätzen zuweisen, die Zugriff auf das Verwaltungskonto gewähren, und Gruppen vermeiden. Wenn Sie Gruppen verwenden, um den Zugriff auf das Verwaltungskonto zu verwalten, stellen Sie sicher, dass der IdP über angemessene Kontrollen verfügt, um einzuschränken, wer

diese Gruppen ändern kann, und stellen Sie sicher, dass Änderungen an diesen Gruppen (oder Änderungen der Anmeldeinformationen für die Benutzer im Verwaltungskonto) protokolliert und gegebenenfalls überprüft 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 delegierte Administratorfunktion von IAM Identity Center aktiviert haben. Wenn Sie beschließen, die IAM Identity Center-Identitätsquelle von einer anderen Quelle auf Active Directory oder von Active Directory auf eine andere Quelle zu ändern, muss sich das Verzeichnis im delegierten IAM Identity Center-Administratorkonto befinden. Wenn Sie möchten, dass sich Ihr Active Directory im Verwaltungskonto befindet, müssen Sie die Einrichtung im Verwaltungskonto vornehmen, da der delegierte Administrator nicht über die erforderlichen Berechtigungen verfügt, um den Vorgang abzuschließen.

Beschränken Sie die IAM Identity Center-Identitätsspeicher-Aktionen im delegierten Administratorkonto auf externe Identitätsquellen

Wenn Sie eine externe Identitätsquelle wie einen IdP oder verwenden, sollten Sie Richtlinien implementieren Directory Service, die die Identitätsspeicher-Aktionen einschränken, die ein IAM Identity Center-Administrator innerhalb des delegierten Administratorkontos ausführen kann. Schreib- und Löschvorgänge sollten sorgfältig abgewogen werden. Im Allgemeinen ist die externe Identitätsquelle die Informationsquelle für Benutzer und ihre Attribute sowie für Gruppenmitgliedschaften. Wenn Sie diese mithilfe des Identitätsspeichers APIs oder der Konsole ändern, werden Ihre Änderungen während normaler Synchronisierungszyklen überschrieben. Überlassen Sie diese Vorgänge am besten der alleinigen Kontrolle Ihrer Identitätsquelle. Dies schützt auch davor, dass ein IAM Identity Center-Administrator Gruppenmitgliedschaften ändert, um Zugriff auf einen der Gruppe zugewiesenen Berechtigungssatz oder eine Anwendung zu gewähren, anstatt die Kontrolle der Gruppenmitgliedschaft Ihrem IdP-Administrator zu überlassen. Sie sollten auch darauf achten, wer SCIM-Trägertoken vom delegierten Administratorkonto aus erstellen kann, da diese es einem Administrator eines Mitgliedskontos ermöglichen könnten, Gruppen und Benutzer über einen SCIM-Client zu ändern.

Es kann vorkommen, dass Schreib- oder Löschvorgänge vom delegierten Administratorkonto aus angemessen sind. Sie können beispielsweise eine Gruppe erstellen, ohne Mitglieder hinzuzufügen, und dann Zuweisungen zu einem Berechtigungssatz vornehmen, ohne darauf warten zu müssen, dass der IdP-Administrator die Gruppe erstellt. Niemand hat Zugriff auf diese Zuweisung, bis der IdP-Administrator die Gruppe bereitstellt und der IdP-Synchronisierungsprozess die Gruppenmitglieder festlegt. Es kann auch sinnvoll sein, einen Benutzer oder eine Gruppe zu löschen, um eine

Anmeldung oder Autorisierung zu verhindern, wenn Sie nicht warten können, bis der IdP-Synchronisierungsprozess den Zugriff des Benutzers oder der Gruppe aufhebt. Ein Missbrauch dieser Berechtigung kann sich jedoch negativ auf die Benutzer auswirken. Bei der Zuweisung von Identitätsspeicherberechtigungen sollten Sie das Prinzip der geringsten Rechte verwenden. Mithilfe einer Service Control Policy (SCP) können Sie steuern, welche Identitätsspeicher-Aktionen von den Administratoren Ihres delegierten Administratorkontos zugelassen werden.

Das folgende Beispiel für SCP verhindert die Zuweisung von Benutzern zu Gruppen über die Identity Store-API und die. Dies wird empfohlen AWS-Managementkonsole, wenn es sich bei Ihrer Identitätsquelle um eine externe Identitätsquelle handelt. Dies hat keinen Einfluss auf die Benutzersynchronisierung von Directory Service oder von einem externen IdP (über SCIM).

> **Note**
>
> Es ist möglich, dass Ihre Organisation, obwohl Sie eine externe Identitätsquelle verwenden, ganz oder teilweise auf den Identitätsspeicher APIs für die Bereitstellung von Benutzern und Gruppen angewiesen ist. Bevor Sie diesen SCP aktivieren, sollten Sie daher sicherstellen, dass Ihr Benutzerbereitstellungsprozess diesen Identity Store-API-Vorgang nicht verwendet. Im nächsten Abschnitt finden Sie außerdem Informationen darüber, wie Sie die Verwaltung von Gruppenmitgliedschaften auf bestimmte Gruppen beschränken können.

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

Wenn Sie verhindern möchten, dass Benutzer nur zu Gruppen hinzugefügt werden, die Zugriff auf das Verwaltungskonto gewähren, können Sie mithilfe des Gruppen-ARN im folgenden Format auf diese spezifischen Gruppen verweisen:`arn:${Partition}:identitystore:::group/${GroupId}`. Dieser und andere im Identity Store verfügbare Ressourcentypen sind unter Ressourcentypen definiert durch AWS Identity Store in der Service Authorization Reference dokumentiert. Sie können auch erwägen, zusätzlichen Identitätsspeicher APIs in den SCP aufzunehmen. Weitere Informationen finden Sie unter Aktionen in der Identity Store-API-Referenz.

Indem Sie Ihrem SCP die folgende Richtlinienerklärung hinzufügen, können Sie die Erstellung von SCIM-Bearer-Token durch den delegierten Administrator verhindern. Sie können dies für beide externen Identitätsquellen anwenden.

> **Note**
>
> Wenn Ihr delegierter Administrator die Benutzerverwaltung mit SCIM einrichten oder die regelmäßige Rotation des SCIM-Bearer-Tokens durchführen muss, müssen Sie vorübergehend den Zugriff auf diese API gewähren, damit der delegierte Administrator diese Aufgaben ausführen kann.

```
{ "Effect": "Deny",
  "Action": ["sso-directory:CreateBearerToken"],
  "Resource": [ "*" ]
}
```

Beschränken Sie die IAM Identity Center-Identitätsspeicher-Aktionen im delegierten Administratorkonto für lokal verwaltete Benutzer

Wenn Sie Ihre Benutzer und Gruppen direkt in IAM Identity Center erstellen, anstatt einen externen IdP oder zu verwenden Directory Service, sollten Sie Vorkehrungen dafür treffen, wer Benutzer erstellen, Passwörter zurücksetzen und die Gruppenmitgliedschaft kontrollieren kann. Diese Aktionen geben dem Administrator umfassende Möglichkeiten, festzulegen, wer sich anmelden kann und wer durch die Mitgliedschaft in Gruppen Zugriff erhält. Diese Richtlinien lassen sich am besten als Inline-Richtlinien innerhalb der Berechtigungssätze implementieren, die Sie für Ihre IAM Identity Center-Administratoren verwenden, und nicht als. SCPs Das folgende Beispiel für eine Inline-Richtlinie verfolgt zwei Ziele. Erstens verhindert sie das Hinzufügen von Benutzern zu bestimmten Gruppen. Sie können dies verwenden, um zu verhindern, dass delegierte Administratoren Benutzer zu Gruppen hinzufügen, die Zugriff auf das Verwaltungskonto gewähren. Zweitens verhindert es die Ausgabe von SCIM-Inhabertoken.

```
{
  "Version": "2012-10-17",
  "Statement": [
  { "Effect": "Deny",
```

```
    "Action": ["identitystore:CreateGroupMembership"],
    "Resource": [ arn:${Partition}:identitystore:::group/${GroupId1},
                  arn:${Partition}:identitystore:::group/${GroupId2}
                ]
   }
  ],
  { "Effect": "Deny",
    "Action": ["sso-directory:CreateBearerToken"],
    "Resource": [ "*" ] }
  ]
}
```

Trennen Sie das IAM Identity Center-Konfigurationsmanagement vom Management PermissionSet

Trennen Sie die administrativen Aufgaben, einschließlich der Änderung der externen Identitätsquelle, der SCIM-Tokenverwaltung und der Konfiguration des Sitzungstimeouts, von den Aufgaben zum Erstellen, Ändern und Zuweisen von Berechtigungssätzen, indem Sie von Ihrem Verwaltungskonto aus unterschiedliche Administratorberechtigungssätze erstellen.

Beschränken Sie die Ausgabe von SCIM-Trägertoken

SCIM-Bearer-Token ermöglichen es einer externen Identitätsquelle, Benutzer, Gruppen und Gruppenmitgliedschaften über das SCIM-Protokoll bereitzustellen, wenn die Identitätsquelle Ihres IAM Identity Center ein externer IdP wie Okta oder Entra ID ist. Sie können den folgenden SCP einrichten, um die Erstellung von SCIM-Trägertoken durch delegierte Administratoren zu verhindern. Wenn Ihr delegierter Administrator die Benutzerverwaltung mit SCIM einrichten oder die regelmäßige Rotation der SCIM-Trägertoken durchführen muss, müssen Sie vorübergehend den Zugriff auf diese API zulassen, damit der delegierte Administrator diese Aufgaben ausführen kann.

```
    { "Effect": "Deny",
      "Action": ["sso-directory:CreateBearerToken"],
      "Resource": [ "*" ]
}
```

Verwenden Sie Berechtigungssatz-Tags und Kontolisten, um die Verwaltung bestimmter Konten zu delegieren

Sie können Berechtigungssätze erstellen, die Sie Ihren IAM Identity Center-Administratoren zuweisen, um zu delegieren, wer Berechtigungssätze erstellen kann und wer welchen Konten welche Berechtigungssätze zuweisen kann. Dazu kennzeichnen Sie Berechtigungssätze mit Tags und verwenden Richtlinienbedingungen in den Berechtigungssätzen, die Sie Ihren Administratoren zuweisen. Sie können beispielsweise Berechtigungssätze erstellen, die es einem Benutzer ermöglichen, Berechtigungssätze zu erstellen, sofern sie auf eine bestimmte Weise gekennzeichnet sind. Sie können auch Richtlinien erstellen, die es einem Administrator ermöglichen, bestimmten Konten Berechtigungssätze zuzuweisen, die mit einem bestimmten Tag versehen sind. Auf diese Weise können Sie die Verwaltung von Konten delegieren, ohne einem Administrator die Rechte zu geben, seinen Zugriff und seine Rechte für das delegierte Administratorkonto zu ändern. Indem Sie beispielsweise Berechtigungssätze kennzeichnen, die Sie nur für das delegierte Administratorkonto verwenden, können Sie eine Richtlinie festlegen, die nur bestimmten Personen die Erlaubnis erteilt, Berechtigungssätze und Zuweisungen zu ändern, die sich auf das delegierte Administratorkonto auswirken. Sie können auch anderen Personen die Erlaubnis geben, eine Liste von Konten außerhalb des delegierten Administratorkontos zu verwalten. Weitere Informationen finden Sie im AWS Sicherheits-Blog unter Delegieren der Verwaltung von Berechtigungssätzen und AWS IAM Identity Center der Kontozuweisung.

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 IAM Identity Center, konfigurierbare AD-Synchronisierung 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-Managementkonsole 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-Managementkonsole 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 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 erweiterter Zugriff für AWS-Konten

Jeder Zugriff auf Ihren ist mit einem gewissen Maß an Rechten AWS-Konto verbunden. Vertrauliche Vorgänge, wie z. B. das Ändern der Konfiguration für eine Produktionsumgebung, erfordern aufgrund ihres Umfangs und ihrer möglichen Auswirkungen eine besondere Behandlung. Temporärer erweiterter Zugriff (auch bekannt als just-in-time Zugriff) 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.

> **Note**
>
> Um die Geschäftskontinuität zu gewährleisten, empfehlen wir Ihnen, den Notfallzugriff auf den AWS-Managementkonsole einzurichten.

Lässt sich in die Lösungen von AWS Sicherheitskompetenzpartnern AWS IAM Identity Center integrieren, um einer Reihe von Kundenanforderungen gerecht zu werden. AWS bestätigt, dass diese Lösungen eine Reihe gängiger temporärer erhöhter Zugriffsanforderungen erfüllen. Wir empfehlen Ihnen, jede Partnerlösung sorgfältig zu prüfen, damit Sie eine Lösung auswählen können, die Ihren individuellen Bedürfnissen und Vorlieben am besten entspricht, einschließlich Ihres Unternehmens, der Architektur Ihrer Cloud-Umgebung und Ihres Budgets.

Zu den validierten Lösungen gehören Apono Access Management Platform, CyberArk Secure Cloud Access, Okta Access Requests und Tenable (zuvor Ermetic).

Partner können mithilfe der Anwendung AWS Security Competency im Partner Center Lösungen nominieren. Weitere Informationen finden Sie unter Partner für AWS Sicherheitskompetenz.

> **Note**
>
> Wenn Sie den ressourcenbasierten Amazon Elastic Kubernetes Service oder AWS Key Management Service verwenden, finden Sie weitere Informationen unter Referenzieren von Berechtigungssätzen in Ressourcenrichtlinien, Amazon EKS-Cluster-Konfigurationszuordnungen und AWS KMS wichtigen Richtlinien, bevor Sie sich für Ihre Lösung entscheiden. just-in-time

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 IAMFullZugriffsrichtlinie oder entsprechende Berechtigungen verfügen, bevor Sie dieses Konto einrichten können. Diese zusätzlichen Sicherheitseinschränkungen sind für keines der Mitgliedskonten in Ihrer AWS Organisation erforderlich.

Themen

- Weisen Sie Benutzer- oder Gruppenzugriff zu AWS-Konten
- Entfernen Sie den Benutzer- und Gruppenzugriff auf ein AWS-Konto

- Widerrufen Sie aktive IAM-Rollensitzungen, die mit Berechtigungssätzen erstellt wurden
- Delegieren Sie, wer Benutzern und Gruppen im Verwaltungskonto Single Sign-On-Zugriff zuweisen kann

Weisen Sie Benutzer- oder Gruppenzugriff 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 unterEinen Berechtigungssatz anzeigen und ändern.

> **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 AWS-Konto neben dem, dem Sie Zugriff zuweisen möchten. Wenn Sie Administratorzugriff für IAM Identity Center einrichten, aktivieren Sie das Kontrollkästchen neben dem Verwaltungskonto.

> **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 zuweisen zu ***AWS-account-name*** "" 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 Berechtigungssätze zuweisen zu ***AWS-account-name*** "" 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 unterErstellen Sie einen

Berechtigungssatz. 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 einreichen an ***AWS-account-name*** "" 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.

   Überlegungen

   - 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 IAMFullZugriffsrichtlinie oder entsprechende Berechtigungen verfügen, bevor Sie dieses Konto einrichten können. Diese zusätzlichen Sicherheitseinschränkungen sind für keines der Mitgliedskonten in Ihrer AWS Organisation erforderlich.

8. 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 das 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.

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.

Entfernen Sie den Benutzer- und Gruppenzugriff auf ein AWS-Konto

Gehen Sie wie folgt vor, um den Single Sign-On-Zugriff auf einen oder mehrere Benutzer und Gruppen in Ihrem verbundenen Verzeichnis zu entfernen. AWS-Konto Sie können aber auch die delete-account-assignment AWS CLI verwenden.

> **Note**
>
> Wenn Sie die Bereitstellung von IAM Identity Center-Benutzern oder -Gruppen aufheben müssen, sollten Sie zunächst alle Zuweisungen von Berechtigungssätzen für Ihre Benutzer und Gruppen entfernen, bevor Sie die Benutzer und Gruppen löschen.

Um 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 den Identitätsspeicher verwenden APIs , 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.

   Nach dem Löschen einer Benutzersitzung verliert der Benutzer sofort den Zugriff auf das AWS Zugangsportal. 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 wählen Sie 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.

Sie können sie auch verwenden, um Richtlinien AWS CLI zu erstellen, ihnen anzuhängen und ihnen Berechtigungssätze zuzuweisen. Im Folgenden sind die Befehle für jeden Schritt aufgeführt:

- Um einen Berechtigungssatz zu erstellen: create-permission-set
- Um ihn an einen Berechtigungssatz AWS Managed Policy anzuhängen: attach-managed-policy-to-permission-set
- Um eine vom Kunden verwaltete Richtlinie an einen Berechtigungssatz anzuhängen: - attach-customer-managed-policy to-permission-set
- So weisen Sie einem Prinzipal einen Berechtigungssatz zu: create-account-assignment

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 unterErstellen Sie einen Berechtigungssatz, 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-Managementkonsole. Zum Beispiel: **`https://console.aws.amazon.com/ec2/`**
        > Weitere Informationen finden Sie unter Stellen Sie den Relay-Status für den schnellen Zugriff auf AWS-Managementkonsole.

    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: Tags aus.
    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 Ressourcen taggen AWS IAM Identity Center.
    7. Überprüfen Sie die von Ihnen getroffenen Auswahlen und wählen Sie dann Erstellen aus.
3. Folgen Sie den Schritten unterWeisen Sie Benutzer- oder Gruppenzugriff 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.

AWS-Konten Mit Berechtigungssätzen verwalten

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.

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 mit nur den erforderlichen Berechtigungen für Ihr Team erstellen.

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 für AWS-Konten.

- 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 im IAM Identity Center.
- 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 Benutzer- oder Gruppenzugriff zu AWS-Konten

Themen

- Vordefinierte Berechtigungen für AWS verwaltete Richtlinien
- Benutzerdefinierte Berechtigungen für AWS verwaltete und vom Kunden verwaltete Richtlinien
- Berechtigungssätze erstellen, verwalten und löschen
- Konfigurieren Sie die Eigenschaften des Berechtigungssatzes

Vordefinierte Berechtigungen für AWS verwaltete Richtlinien

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 für AWS verwaltete und vom Kunden verwaltete Richtlinien

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

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.

> **Note**
>
> Wenn eine vom Kunden verwaltete Richtlinie an einen Berechtigungssatz angehängt wird, wird beim Namen der Richtlinie nicht zwischen Groß- und Kleinschreibung unterschieden.

Weitere Informationen finden Sie unter Vom Kunden verwaltete Richtlinien im IAM-Benutzerhandbuch.

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, dürfen Ihre Eingebundene RichtlinienKundenverwaltete Richtlinien, und AWS verwaltete Richtlinien keine Berechtigungen gewähren, die die von Ihrer 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. AWS-Konten Mit Berechtigungssätzen verwalten

> **Note**
>
> In der IAM Identity Center-Konsole können Sie nach Berechtigungssätzen suchen und sie nach Namen sortieren.

Beachten Sie bei der Erstellung von Berechtigungssätzen die folgenden Überlegungen:

- Instanz der Organisation

  Um Berechtigungssätze verwenden zu können, müssen Sie eine Organisationsinstanz von IAM Identity Center verwenden. Weitere Informationen finden Sie unter Organisations- und Kontoinstanzen von IAM Identity Center.

- 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 ihrem Netzwerk verbinden AWS-Konto und die AWS-Managementkonsole 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. Als bewährte Sicherheitsmaßnahme empfehlen wir Ihnen, die Sitzungsdauer nicht länger als für die Ausführung der Rolle nötig festzulegen. 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 für AWS-Konten.

- 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 im IAM Identity Center.

- 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

Erstellen Sie einen Berechtigungssatz

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.

> **Note**
>
> Um Berechtigungssätze verwenden zu können, müssen Sie eine Organisationsinstanz von IAM Identity Center verwenden. Weitere Informationen finden Sie unter Organisations- und Kontoinstanzen von IAM Identity Center.

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 im AWS Identity and Access Management Benutzerhandbuch unter AWS Verwaltete Richtlinien für Aufgabenfunktionen und AWS Verwaltete Richtlinien.
     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“ aus, 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.

> **Note**
>
> Die Namen der Berechtigungssätze müssen innerhalb Ihrer IAM Identity Center-Instanz eindeutig sein.

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 für AWS-Konten.
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 für den schnellen Zugriff auf AWS-Managementkonsole.

> **Note**
>
> Die Relay-State-URL muss sich innerhalb von befinden AWS-Managementkonsole. Zum Beispiel:
> **`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 Ressourcen taggen AWS IAM Identity Center.

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 Weisen Sie Benutzer- oder Gruppenzugriff zu AWS-Konten.

Einen Berechtigungssatz anzeigen und ändern

Sie können Berechtigungssätze verwenden, um Benutzern Zugriff auf zu AWS-Konten gewähren. Sie können einen Berechtigungssatz mit der AWS IAM Identity Center Konsole anzeigen und ändern. In der IAM Identity Center-Konsole können Sie Berechtigungssätze nach Namen suchen und sortieren. Weitere Informationen zu Berechtigungssätzen und deren Verwendung in IAM Identity Center finden Sie unter. the section called “Berechtigungssätze”

Für die Verwaltung des Benutzerzugriffs auf Anwendungen sind keine Berechtigungssätze erforderlich.

> **Note**
>
> Um Berechtigungssätze verwenden zu können, müssen Sie eine Organisationsinstanz von IAM Identity Center verwenden. Weitere Informationen finden Sie unter Organisations- und Kontoinstanzen von IAM Identity Center.

Zuweisungen von Berechtigungssätzen anzeigen

Gehen Sie wie folgt vor, um den angewendeten Berechtigungssatz in der AWS IAM Identity Center Konsole anzuzeigen.

All AWS-Konten where a permission set is provisioned

Gehen Sie wie folgt vor, um alle Zuweisungen für einen Berechtigungssatz anzuzeigen:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS IAM Identity Center Konsole unter https://console.aws.amazon.com/singlesignon/.
2. Wählen Sie unter Berechtigungen für mehrere Konten die Option Berechtigungssätze aus.
3. Wählen Sie auf der Seite Berechtigungssätze den Berechtigungssatz aus, den Sie anzeigen möchten.
4. Sobald Sie sich auf der Seite mit den ausgewählten Berechtigungssätzen befinden, können Sie auf der Registerkarte Konten die Konten sehen, für die der Berechtigungssatz verwendet wird. Sie können das Konto auswählen, um zu sehen, wie der Berechtigungssatz innerhalb des Kontos bereitgestellt wird. Sie können Richtlinien löschen, bearbeiten und an den Berechtigungssatz anhängen.

All permission sets for an AWS-Konto

Gehen Sie wie folgt vor, um alle Zuweisungen für einen Berechtigungssatz anzuzeigen:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS IAM Identity Center Konsole unter https://console.aws.amazon.com/singlesignon/.
2. Wählen Sie unter Berechtigungen für mehrere Konten die Option AWS-Konten. Wählen Sie das Konto aus, für das Sie die bereitgestellten Berechtigungssätze anzeigen möchten.
3. Sobald Sie sich auf der ausgewählten AWS-Konto Seite befinden, können Sie auf der Registerkarte Berechtigungssätze die verschiedenen Berechtigungssätze einsehen, die den ausgewählten AWS-Konto Benutzern zugewiesen sind. Sie können den Hyperlink zum Berechtigungssatz auswählen, um mehr über den Berechtigungssatz zu erfahren.

All applied permission sets to users and groups

Gehen Sie wie folgt vor, um alle Berechtigungssätze anzuzeigen, die Benutzern oder Gruppen zugewiesen sind:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS IAM Identity Center Konsole unter https://console.aws.amazon.com/singlesignon/.
2. Wählen Sie unter Dashboard entweder Benutzer oder Gruppen aus, um die Benutzer oder Gruppen von IAM Identity Center anzuzeigen.

    a. Wählen Sie auf der Seite Benutzer den Benutzer aus, für den Sie die angewendeten Berechtigungssätze sehen möchten. Wählen Sie als Nächstes die AWS-KontenRegisterkarte und anschließend den AWS-Konto Abschnitt AWS Kontozugriff

aus. Sie können die angewendeten Berechtigungssätze und die AWS-Konto für den ausgewählten Benutzer verwendeten Berechtigungssätze sehen.

b. Wählen Sie auf der Gruppenseite die Gruppe aus, für die Sie die angewendeten Berechtigungssätze anzeigen möchten. Wählen Sie als Nächstes die AWS-KontenRegisterkarte und anschließend den AWS-Konto Abschnitt AWS-Konto Zugriff aus. Sie können die angewendeten Berechtigungssätze und die AWS-Konto für die ausgewählte Gruppe verwendeten Berechtigungssätze sehen.

Ändern Sie einen Berechtigungssatz

Gehen Sie wie folgt vor, um einen Berechtigungssatz mit der IAM Identity Center-Konsole zu ändern. Sie können Berechtigungssätze für Benutzer oder Gruppen hinzufügen oder daraus entfernen.

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS IAM Identity Center Konsole unter https://console.aws.amazon.com/singlesignon/.
2. Wählen Sie unter Berechtigungen für mehrere Konten die Option AWS-Konten.
3. Auf der AWS-KontoSeite wird eine Strukturansicht Ihrer Organisation angezeigt. Wählen Sie den Namen des Berechtigungssatzes AWS-Konto aus, für den Sie den Berechtigungssatz ändern möchten.
4. Wählen Sie auf der Übersichtsseite von unter Zugewiesene Benutzer und Gruppen den Benutzernamen oder Gruppennamen des Berechtigungssatzes aus, den Sie ändern möchten. AWS-Konto Wählen Sie dann Berechtigungssätze ändern aus.
5. Nehmen Sie die gewünschten Änderungen am Berechtigungssatz vor und wählen Sie dann Änderungen speichern.
6. Navigieren Sie zur Registerkarte Berechtigungssätze, wählen Sie den kürzlich geänderten Berechtigungssatz aus und wählen Sie Aktualisieren aus.
7. Wählen Sie auf der Seite „Berechtigungen aktualisieren“ die Option Aktualisieren aus.

Delegieren Sie die Verwaltung von Berechtigungssätzen

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) der 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.

> **Note**
>
> Um Berechtigungssätze verwenden zu können, müssen Sie eine Organisationsinstanz von IAM Identity Center verwenden. Weitere Informationen finden Sie unter Organisations- und Kontoinstanzen von IAM Identity Center.

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 IAM Identity Center-Ressourcen wird zwischen Groß- und Kleinschreibung ARNs 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:${Partition}:sso:::permissionSet/${InstanceId}/${PermissionSetId}`	`aws:ResourceTag/${TagKey}`
Account	`arn:${Partition}:sso:::account/${AccountId}`	Nicht zutreffend

Verwenden Sie IAM-Richtlinien in Berechtigungssätzen

In haben Sie gelerntErstellen Sie einen Berechtigungssatz, 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.

Überlegungen

- Um Berechtigungssätze verwenden zu können, müssen Sie eine Organisationsinstanz von IAM Identity Center verwenden. Weitere Informationen finden Sie unter Organisations- und Kontoinstanzen von IAM Identity Center.
- Bevor Sie Ihrem Berechtigungssatz IAM-Richtlinien zuweisen, müssen Sie Ihr Mitgliedskonto vorbereiten. Der Name einer IAM-Richtlinie in Ihrem Mitgliedskonto muss 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.

  > **Note**
  >
  > Wenn eine vom Kunden verwaltete Richtlinie an einen Berechtigungssatz angehängt wird, wird beim Namen der Richtlinie nicht zwischen Groß- und Kleinschreibung unterschieden.

- Die Berechtigungen, die die Richtlinie gewährt, müssen den Konten nicht exakt entsprechen.

Weisen Sie einem Berechtigungssatz eine IAM-Richtlinie zu

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 unterErstellen Sie einen Berechtigungssatz.
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.

Entfernen Sie die Berechtigungssätze im IAM Identity Center

In der IAM Identity Center-Konsole können Sie einen Berechtigungssatz für Benutzer und Gruppen von IAM Identity Center entfernen. Sie können einen Berechtigungssatz auch aus einem entfernen. AWS-Konto Weitere Informationen zu Berechtigungssätzen und deren Verwendung in IAM Identity Center finden Sie unterAWS-Konten Mit Berechtigungssätzen verwalten.

> **Note**
>
> Um Berechtigungssätze verwenden zu können, müssen Sie eine Organisationsinstanz von IAM Identity Center verwenden. Weitere Informationen finden Sie unter Organisations- und Kontoinstanzen von IAM Identity Center.

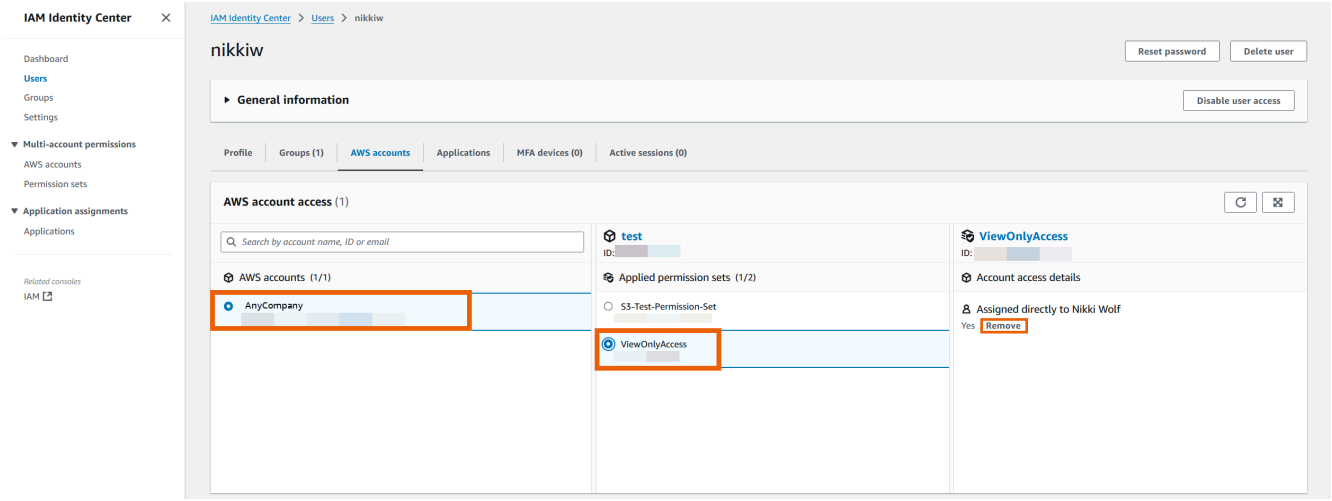
Remove permission set from a user

Entfernen Sie den Berechtigungssatz von einem Benutzer

Gehen Sie wie folgt vor, um mit der IAM Identity Center-Konsole einen Berechtigungssatz von einem Benutzer zu entfernen.

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS IAM Identity Center Konsole unter https://console.aws.amazon.com/singlesignon/.
2. Wählen Sie unter IAM Identity Center die Option Benutzer aus.
3. Wählen Sie den Benutzernamen des Benutzers aus, für den Sie einen Berechtigungssatz entfernen möchten.

4. Wählen Sie auf der Seite mit den Benutzerdetails die AWS-KontenRegisterkarte aus. Wählen Sie unter AWS-Konto Zugriff Ihre aus AWS-Konto.
5. Im rechten Bereich werden die angewendeten Berechtigungen für den ausgewählten Benutzer angezeigt. Wählen Sie den Berechtigungssatz aus, den Sie entfernen möchten. Wählen Sie unter Kontozugriffsdetails die Option Entfernen aus.
6. In einem Dialogfeld werden Sie gefragt, ob Sie diesen Berechtigungssatz entfernen möchten. Wählen Sie Entfernen aus.

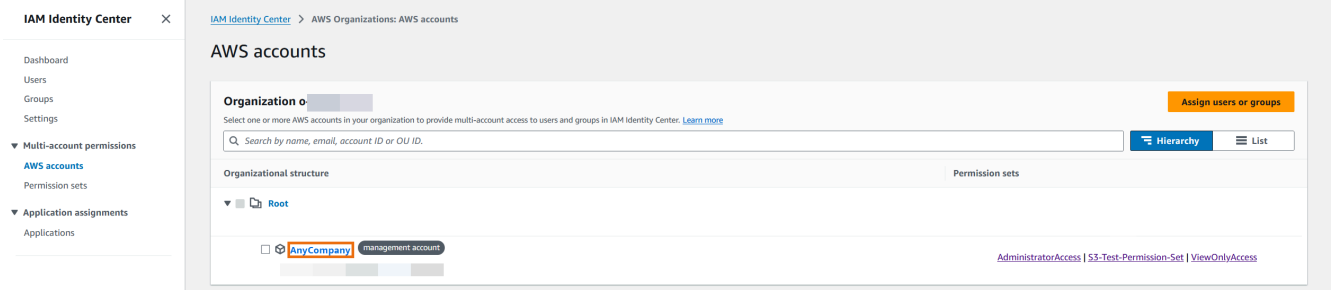


Remove permission set from a group

Entfernen Sie den Berechtigungssatz aus einer Gruppe

Gehen Sie wie folgt vor, um mit der IAM Identity Center-Konsole einen Berechtigungssatz aus einer Gruppe zu entfernen.

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS IAM Identity Center Konsole unter https://console.aws.amazon.com/singlesignon/.
2. Wählen Sie unter Berechtigungen für mehrere Konten die Option aus AWS-Konten. Wählen Sie den Link zu Ihrem Verwaltungskonto aus.



3. Wählen Sie auf der Registerkarte Zugewiesene Benutzer und Gruppen die Gruppe aus, aus der Sie den Berechtigungssatz entfernen möchten, und wählen Sie dann Berechtigungssatz ändern aus.
4. Löschen Sie auf der Seite Berechtigungssätze ändern den Berechtigungssatz, den Sie entfernen möchten, und wählen Sie dann Änderungen speichern aus.

Remove permission set from an AWS-Konto

Gehen Sie wie folgt vor, um AWS-Konto mit der IAM Identity Center-Konsole einen Berechtigungssatz aus der zu entfernen.

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS IAM Identity Center Konsole unter https://console.aws.amazon.com/singlesignon/.
2. Wählen Sie unter Berechtigungen für mehrere Konten die Option aus AWS-Konten. Wählen Sie den Namen des Berechtigungssatzes AWS-Konto aus, für den Sie den Berechtigungssatz entfernen möchten.
3. Wählen Sie auf der Übersichtsseite von die AWS-Konto Registerkarte Berechtigungssätze aus. Wählen Sie den Berechtigungssatz aus, den Sie entfernen möchten. Wählen Sie dann Entfernen aus.
4. 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.

Löschen Sie die Berechtigungssätze in IAM Identity Center

Bevor Sie einen Berechtigungssatz aus IAM Identity Center löschen können, sollten Sie ihn aus allen entfernen, AWS-Konten die den Berechtigungssatz verwenden. Informationen zum Überprüfen vorhandener Benutzer- und Gruppenzugriffe finden Sie unterEinen Berechtigungssatz anzeigen und ändern.

Überlegungen

- Um Berechtigungssätze verwenden zu können, müssen Sie eine Organisationsinstanz von IAM Identity Center verwenden. Weitere Informationen finden Sie unter Organisations- und Kontoinstanzen von IAM Identity Center.
- Informationen zum Widerrufen einer aktiven Berechtigungssatz-Sitzung finden Sie unterthe section called “Beenden Sie aktive Sitzungen für Workforce-Benutzer”.

- Sie sollten die Berechtigungssätze und Anwendungszuweisungen von Benutzern oder Gruppen entfernen, die Sie löschen möchten, bevor Sie sie löschen. Andernfalls verfügen Sie in IAM Identity Center über nicht zugewiesene und ungenutzte Berechtigungssätze und Anwendungen.

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.

> **Important**
>
> 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 unterEinen Berechtigungssatz anzeigen und ändern.

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 Administratoren die folgenden Konfigurations- und Verwaltungsaufgaben ausführen, um den Benutzerzugriff und die Sitzungsdauer zu steuern.

Aufgabe	Weitere Informationen
Administratoren können die maximale Dauer für Benutzersitzungen festlegen, wenn sie über IAM Identity Center auf AWS Ressourcen zugreifen.	Legen Sie die Sitzungsdauer fest für AWS-Konten

Aufgabe	Weitere Informationen
Administratoren können die Landingpage anpassen, die Benutzern nach erfolgreicher Authentifizierung über IAM Identity Center angezeigt wird.	Stellen Sie den Relay-Status für den schnellen Zugriff auf AWS-Managementkonsole
Stellen Sie sicher, dass Benutzer keinen Zugriff mehr auf AWS Ressourcen haben, wenn ihre Berechtigungen widerrufen werden.	Verwenden Sie eine Ablehnungsrichtlinie, um aktiven Benutzerberechtigungen zu entziehen

Legen Sie die Sitzungsdauer fest für AWS-Konten

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

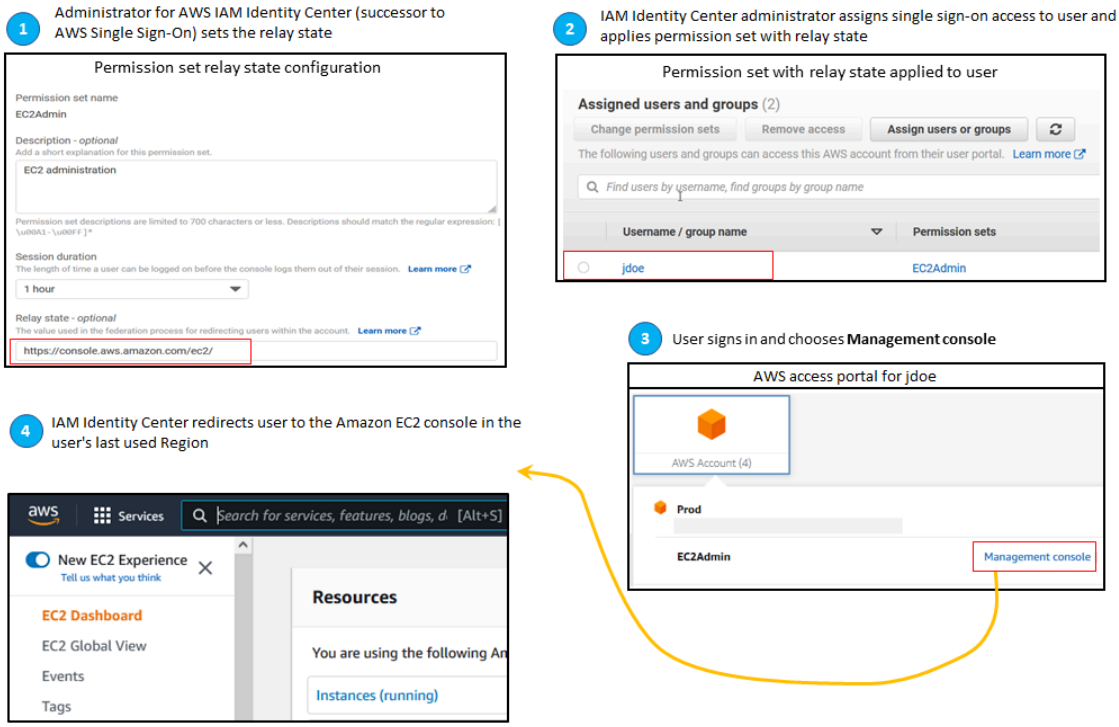
1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie unter Berechtigungen für mehrere Konten die Option Berechtigungssätze aus.
3. Wählen Sie den Namen des Berechtigungssatzes aus, für den Sie die Sitzungsdauer ändern möchten.
4. Wählen Sie auf der Detailseite für den Berechtigungssatz rechts 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 für den schnellen Zugriff auf AWS-Managementkonsole

Wenn sich ein Benutzer beim AWS Zugriffsportal anmeldet, ein Konto auswählt und dann anhand des zugewiesenen Berechtigungssatzes AWS die Rolle auswählt, leitet IAM Identity Center den Browser des Benutzers standardmäßig an den weiter. AWS-Managementkonsole 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 EC2 Amazon-Konsolen-URL (**`https://console.aws.amazon.com/ec2/`**) setzen, um den Benutzer zu dieser Konsole umzuleiten, wenn er die EC2 Amazon-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 EC2 Amazon-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 EC2 Amazon-Konsole in der Region USA Ost (Ohio) (us-east-2) umzuleiten, geben Sie die URL für die EC2 Amazon-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`**

Konfigurieren Sie den Relay-Status

Gehen Sie wie folgt vor, um die Relay-Status-URL für einen Berechtigungssatz 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. Zum Beispiel:

   `https://console.aws.amazon.com/ec2/`

   > **Note**
   >
   > Die Relay-Status-URL muss sich innerhalb von befinden AWS-Managementkonsole.

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 unter:
>
> - 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. Dadurch wird ein böswilliger Akteur, der gestohlene Anmeldeinformationen aktiv missbraucht, entfernt. 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 the section called “Beenden Sie aktive Sitzungen für Workforce-Benutzer” 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.

JSON

```
{
    "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 des Identitätsspeichers abrufen. APIs

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 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 im Bedingungsblock eine Liste mit Werten 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-Cluster-Konfigurationszuordnungen und AWS KMS wichtigen Richtlinien

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.amazonaws.com/` *`aws-region`* `/AWSReservedSSO_` *`permission-set-name_unique-suffix`*

Wenn Ihre Identitätsquelle in IAM Identity Center in us-east-1 gehostet wird, gibt es keine *`aws-region`* im ARN. Der vollständige Name und der 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.amazonaws.com/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) -Cluster, wenn Sie den `aws-auth ConfigMap` für den Clusterzugriff verwenden.
- In einer ressourcenbasierten Richtlinie für einen AWS Key Management Service () -Schlüssel.AWS KMS Diese Richtlinie wird auch als Schlüsselrichtlinie bezeichnet.

> **Note**
>
> Wir empfehlen Ihnen, Amazon EKS-Zugriffseinträge zu verwenden, um den Zugriff auf Ihre Amazon EKS-Cluster zu verwalten. Auf diese Weise können Sie IAM-Berechtigungen verwenden, um die Principals zu verwalten, die Zugriff auf einen Amazon EKS-Cluster haben. Durch die Verwendung von Amazon EKS-Zugriffseinträgen können Sie einen IAM-Prinzipal mit Amazon EKS-Berechtigungen verwenden, um den Zugriff auf einen Cluster wiederherzustellen, ohne Kontakt aufzunehmen Support.

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 nicht über eine Backup-IAM-Rolle mit Berechtigungen zum Aktualisieren der `aws-auth ConfigMap` oder der AWS KMS Schlüsselrichtlinie verfügen, wenden Sie sich an uns, Support um wieder Zugriff auf diese Ressourcen zu erhalten.

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-Cluster, die verwenden **`aws-auth ConfigMap`** und AWS KMS: Fügen Sie eine in IAM erstellte Rolle hinzu.

Wenn Sie bei ARNs Berechtigungssätzen in einem `aws-auth ConfigMap` Amazon EKS-Cluster oder in Schlüsselrichtlinien für AWS KMS Schlüssel auf Rollen 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.

JSON

```
{
  "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 Benutzerattribute hinweg zu verwalten, die aus AWS-Konten 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 Aufgabenfunktionen 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 des

IAM Identity Center finden Sie CreateInstanceAccessControlAttributeConfigurationim IAM Identity Center APIs API-Referenzhandbuch.

Themen

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 Ressource n hinzufügen können. Um ABAC in IAM Identity Center zu implementieren, müssen Sie zunächst allen AWS Ressourcen, für die Sie ABAC implementieren möchten, Tags hinzufügen.	• 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-Identitätsq uelle für ABAC in verwenden. AWS	• Verwaltung Ihrer Identität squelle
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	• Auswahl von Attributen, wenn Sie einen externen

Schritt	Aufgabe	Referenz
	übergebene Attribute verwenden oder Attribute aus IAM Identity Center auswählen möchten.	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 spezifisc hen IdP an.	• Tutorials zu Identitätsquellen im IAM Identity Center
	• 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.	• Stellen Sie Benutzer und Gruppen von einem externen Identitätsanbieter mithilfe von SCIM bereit • Unterstützte externe Identitätsanbieter-Attribute
	• 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 zwischen IAM Identity Center und Microsoft AD

Schritt	Aufgabe	Referenz
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
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 in 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 Benutzer- oder Gruppenzugriff 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 als Nächstes 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 zwischen IAM Identity Center und Microsoft AD

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 das IAM Identity Center übertragen werden, hat der Wert der SCIM-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 Tutorials zu Identitätsquellen im IAM Identity Center 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 Identitätsanbieter-Attribute.

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 in IAM Identity Center Berechtigungsrichtlinien für ABAC

Aktivieren und konfigurieren Sie Attribute für die Zugriffskontrolle

Um die attributebasierte Zugriffskontrolle (ABAC) verwenden zu können, müssen Sie sie zunächst entweder auf der Einstellungsseite der IAM Identity Center-Konsole oder in der IAM Identity Center-API aktivieren. Unabhängig von der Identitätsquelle können Sie jederzeit Benutzerattribute aus dem Identity Store für die Verwendung in ABAC konfigurieren. In der Konsole können Sie dies tun, indem Sie auf der Seite Einstellungen zur Registerkarte Attribute für die Zugriffskontrolle navigieren. Wenn Sie einen externen Identitätsanbieter (IdP) als Identitätsquelle verwenden, haben Sie auch die Möglichkeit, Attribute vom externen IdP in SAML-Assertionen zu empfangen. In diesem Fall müssen Sie den externen IdP so konfigurieren, dass er die gewünschten Attribute sendet. Wenn ein Attribut aus einer SAML-Assertion auch als ABAC-Attribut in IAM Identity Center definiert ist, sendet IAM Identity Center den Wert aus seinem Identity Store als Sitzungs-Tag bei der Anmeldung an einen. AWS-Konto

> **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.

Themen

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

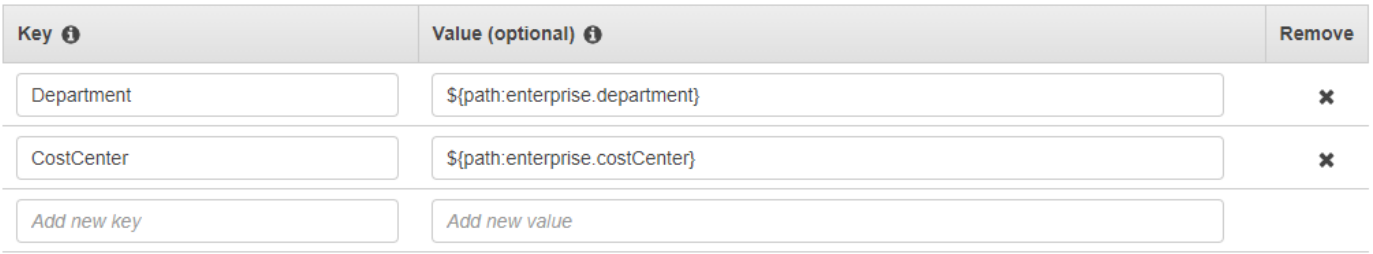
1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie Einstellungen
3. Suchen Sie auf der Seite Einstellungen das Informationsfeld Attribute für die Zugriffskontrolle und wählen Sie dann Aktivieren aus. Fahren Sie mit dem nächsten Verfahren fort, um es zu konfigurieren.

Wählen Sie Ihre Attribute für die Zugriffskontrolle

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 einwertiges Attribut 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 zwischen dem IAM Identity Center

und dem Verzeichnis externer Identitätsanbieter. 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 and/or ressourcenbasierten Richtlinien für Berechtigungssätze hinzu. Dies ist erforderlich, damit Sie Benutzeridentitäten Zugriff auf Ressourcen gewähren können. AWS Weitere Informationen finden Sie unter Erstellen Sie in 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 aus.
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 verwalten“ die Option Deaktivieren aus.
5. Überprüfen Sie im Dialogfeld „Attribute für die Zugriffskontrolle deaktivieren“ die Informationen, geben Sie sie ein**`DISABLE`**, und wählen Sie dann Bestätigen.

> **Important**
>
> Dieser Schritt löscht alle Attribute und beendet die Verwendung von Attributen für die Zugriffskontrolle beim Zusammenschluss, AWS-Konten unabhängig davon, ob Attribute in SAML-Assertionen eines externen Identitätsquellenanbieters vorhanden sind.

Erstellen Sie in 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, leitet IAM Identity Center den Attributwert des authentifizierten Benutzers zur Verwendung bei der Richtlinienbewertung an IAM weiter.

aws:PrincipalTag-Bedingungsschlüssel

Mithilfe des Bedingungsschlüssels können Sie Zugriffskontrollattribute in Ihren Berechtigungssätzen verwenden, um `aws:PrincipalTag` Zugriffskontrollregeln zu erstellen. In der folgenden Richtlinie 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.

JSON

```
{
    "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 im IAM-Benutzerhandbuch unter aws:PrincipalTagund EC2: Starten oder Beenden von Instances auf der Grundlage übereinstimmender Haupt- und Ressourcen-Tags.

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.

Grundlegendes zu serviceverknüpften Rollen in IAM Identity Center

Bei dienstbezogenen Rollen handelt es sich um vordefinierte IAM-Berechtigungen, mit denen IAM Identity Center delegieren und durchsetzen kann, 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 Konfigurieren Sie den Zugriff 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.

Hinweise

- Wenn Sie mit dem 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.

Einrichtung und Nutzung des AWS Zugangsportals

Das AWS Zugriffsportal verbindet Ihre Belegschaft über IAM Identity Center mit Cloud-Anwendungen. AWS-Konten Administratoren konfigurieren das Portal und verwalten den Benutzerzugriff, während sich Endbenutzer einmal anmelden, um problemlos auf alle autorisierten Ressourcen zugreifen zu können.

Das AWS Zugriffsportal bietet Single Sign-On-Zugriff auf:

- AWS-Konten in Ihrer Organisation.
- AWS verwaltete Anwendungen wie Amazon Quick Suite und Amazon Q Developer.
- Cloud-Anwendungen wie Office 365, Concur, Salesforce und andere.

Wenn sich Benutzer im Portal anmelden, finden sie die AWS-Konten Anwendungen, für die sie ohne zusätzliche Anmeldung autorisiert sind.

Erste Schritte mit dem AWS Zugriffsportal

Für Administratoren:

Sie benötigen Administratorzugriff auf Ihre Organisationsinstanz oder Kontoinstanz von IAM Identity Center, um das AWS Zugriffsportal zu konfigurieren und den Benutzerzugriff zu verwalten.

1. Passen Sie optional die URL des AWS Zugriffsportals an.
2. Weisen Sie Benutzerzugriff auf AWS-Konten Anwendungen zu. Zugewiesene AWS Ressourcen werden im Portal angezeigt.

Für Endbenutzer:

Ihr Administrator muss die Einrichtung des AWS Access-Portals abgeschlossen und Ihnen Ihre Portal-URL und Ihre Anmeldeinformationen zur Verfügung gestellt haben.

1. Sie erhalten Ihre Portal-URL von Ihrem Administrator (in der Regel`https://your-company.awsapps.com/start`).
2. Melden Sie sich mit den von Ihrem Administrator bereitgestellten Anmeldeinformationen an.
3. Greifen Sie in Ihrem Portal auf Ihre Ressourcen zu.

Konfigurieren Sie das AWS Zugriffsportal

Als Administrator können Sie das AWS Zugriffsportal an die Bedürfnisse Ihres Unternehmens anpassen und sicherstellen, dass Benutzer problemlos auf ihre autorisierten Ressourcen zugreifen können.

Was können Sie konfigurieren

AWS Aktivierung des Zugriffsportals: Richten Sie den ersten Benutzerzugriff auf das AWS Zugriffsportal ein, einschließlich der Aktivierung von Benutzeranmeldedaten und der Erstanmeldung.

URL des benutzerdefinierten AWS Zugriffsportals (optional): Personalize Sie die URL des AWS Zugriffsportals Ihrer Organisation vom Standardformat (`d-xxxxxxxxxx.awsapps.com/start`) bis hin zu einer besser erkennbaren Subdomain (`your-company.awsapps.com/start`).

Bevor Sie beginnen

Stellen Sie sicher, dass Sie Administratorzugriff auf IAM Identity Center haben, stellen Sie sicher, dass IAM Identity Center entweder als Organisationsinstanz oder als Kontoinstanz eingerichtet ist, und planen Sie Ihren benutzerdefinierten Subdomänennamen (dies ist eine einmalige Konfiguration, die später nicht geändert werden kann).

Nach der Konfiguration können Benutzer über die benutzerdefinierte URL AWS auf das Zugriffsportal zugreifen und den Aktivierungsprozess verfolgen, den Sie für Ihre Organisation eingerichtet haben.

Themen

- Aktivierung des AWS Zugriffsportals für IAM Identity Center-Erstbenutzer
- Anpassen der URL des AWS Access-Portals
- Bestätigen Sie, dass sich Benutzer beim AWS Access-Portal anmelden können

Aktivierung des AWS Zugriffsportals für IAM Identity Center-Erstbenutzer

Wenn Sie zum ersten Mal versuchen, sich beim AWS Zugangsportal anzumelden, finden Sie in Ihren E-Mails Anweisungen zur Aktivierung Ihrer Benutzeranmeldeinformationen.

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 erhalten haben, öffnen Sie diese und wählen Sie Einladung annehmen. Geben Sie auf der Anmeldeseite für neue Benutzer ein Passwort ein, bestätigen Sie es und wählen Sie dann Neues Passwort einrichten. 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 unter manuell beim AWS Access Portal anmeldenMelden Sie sich beim AWS Zugangsportal an.

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.

Bestätigen Sie, dass sich Benutzer beim AWS Access-Portal anmelden können

Die folgenden Schritte dienen dazu, dass der IAM Identity Center-Administrator bestätigt, dass sich der IAM Identity Center-Benutzer beim AWS Zugriffsportal anmelden und auf das zugreifen kann. AWS-Konto

Melden Sie sich beim Zugriffsportal an AWS

1. Führen Sie einen der folgenden Schritte aus, um sich bei der anzumelden AWS-Managementkonsole.
   - 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.

6. Suchen Sie auf der Registerkarte Konten nach Ihrem Konto AWS-Konto und erweitern Sie es.
7. 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.
8. 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 Benutzer- oder Gruppenzugriff 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-Managementkonsole 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. Verwenden Sie diese nur, 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.

Verwenden Sie das Zugriffsportal AWS

Sie können mehrere Anwendungen starten, indem Sie im Portal die Registerkarte AWS-Konto oder Anwendung 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.

Wie benutzt man das Zugangsportal AWS

Um das AWS Zugangsportal zu verwenden:

1. Holen Sie sich Ihre Portal-URL von Ihrem Administrator (sieht normalerweise so aus`https://your-company.awsapps.com/start`).
2. Melden Sie sich mit den von Ihrem Administrator bereitgestellten Anmeldeinformationen an.
3. Wählen Sie die Konten und Anwendungen in Ihrem Portal aus, auf die Sie zugreifen möchten.

Ihr Administrator steuert basierend auf Ihrer Rolle und Ihren Berechtigungen, was Sie im Portal sehen. 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

- Ihre aktive Sitzung anzeigen und beenden

Melden Sie sich beim AWS Zugangsportal an

Das AWS Zugriffsportal bietet Benutzern von IAM Identity Center über ein Webportal Single Sign-On-Zugriff auf alle ihnen zugewiesenen AWS-Konten Anwendungen. Im Folgenden wird beschrieben, wie Sie sich beim AWS Zugriffsportal anmelden können. Außerdem erhalten Sie Tipps zur Anmeldung und wie Sie sich vom AWS Zugriffsportal abmelden.

Voraussetzungen

IAM Identity Center muss aktiviert sein, um das AWS Zugriffsportal nutzen zu können. Weitere Informationen finden Sie unter IAM Identity Center aktivieren.

> **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.

Melden Sie sich im AWS Zugangsportal an

Um sich beim AWS Zugangsportal anzumelden

1. Fügen Sie in Ihrem Browserfenster die Anmelde-URL ein, die Sie erhalten haben, und wählen Sie Enter. Die URL sieht aus wie `d-xxxxxxxxxx.awsapps.com/start` oder *`your_subdomain`*`.awsapps.com/start`. Wir empfehlen, diesen Link zum Portal jetzt als Lesezeichen zu setzen, sodass Sie später schnell darauf zugreifen können.
2. Melden Sie sich mit Ihren standardmäßigen Firmenanmeldedaten an.

   > **Note**
   >
   > Wenn Ihr Administrator Ihnen per E-Mail ein Einmalpasswort (OTP) gesendet hat und Sie sich zum ersten Mal anmelden, geben Sie dieses Passwort ein. Nachdem Sie angemeldet sind, müssen Sie ein neues Passwort für future Anmeldungen erstellen.

Wenn Sie zur Eingabe eines Bestätigungscodes aufgefordert werden, überprüfen Sie Ihre E-Mails, kopieren Sie den Code und fügen Sie ihn auf der Anmeldeseite ein.

> **Note**
>
> Bestätigungscodes werden normalerweise per E-Mail gesendet, aber die Zustellungsmethode kann variieren. Weitere Einzelheiten erhalten Sie von Ihrem Administrator.

3. Sobald Sie angemeldet sind, können Sie auf alle AWS-Konto Anwendungen zugreifen, die im Portal angezeigt werden.

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-Codes 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.

Das Benutzerkennwort Ihres AWS Access-Portals 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-Managementkonsole, 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-Mail. 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 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 oder AWS CLIAWS SDKs

Sie können programmgesteuert auf AWS Dienste zugreifen, indem Sie die AWS Command Line Interface AWS Software Development Kits (SDKs) mit Benutzeranmeldedaten aus dem 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 die Anmeldeinformationen, die auch als IAM Identity Center-Benutzeranmeldedaten bezeichnet werden, dann im AWS CLI oder verwenden, AWS SDKs 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 den für den programmgesteuerten AWS SDKs Zugriff auf AWS Dienste verwenden, wird durch das Befolgen der Verfahren in diesem Thema auch direkt die Authentifizierung für eingerichtet. AWS SDKs Weitere Informationen zu finden Sie im AWS SDKs Referenzhandbuch AWS SDKs und im Tools-Referenzhandbuch.

> **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 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 Benutzer- oder Gruppenzugriff 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 für AWS-Konten.

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 Mit diesem Befehl können Sie automatisch auf jede Rolle zugreifen, 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 Benutzer- oder Gruppenzugriff 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 einem bestimmten Berechtigungssatz in einer bestimmten Rolle zugeordnet 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 Access Portal 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.

   > **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 Benutzer- oder Gruppenzugriff 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 unter Dateien mit gemeinsam genutzten Konfigurationen und Anmeldeinformationen im AWS SDKs Referenzhandbuch zu Tools. 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 für 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-Managementkonsole Zielen erstellen

Im AWS Zugriffsportal erstellte Shortcut-Links führen IAM Identity Center-Benutzer zu einem bestimmten Ziel in AWS-Managementkonsole, 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-Managementkonsole (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 Kurzlink AWS-Managementkonsole 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 für den schnellen Zugriff auf AWS-Managementkonsole
- AWS-Managementkonsole Zuhause. Das Standardziel, falls 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 Konten 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. Verknüpfungen 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 keine URL eingeben, 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-Managementkonsole 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`

Ihr Gerät für MFA registrieren

Verwenden Sie für Benutzer im Identity Center-Verzeichnis das folgende Verfahren im AWS Zugriffsportal, um Ihr neues Gerät für die Multi-Faktor-Authentifizierung (MFA) zu registrieren.

> **Important**
>
> MFA in IAM Identity Center wird derzeit nicht für externe Identitätsanbieter unterstützt.

Bevor Sie beginnen

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.

Registrieren Sie Ihr Gerät

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 Zugangsportal 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 ist je nach Browser oder Plattform unterschiedlich. 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“.

Ihre aktive Sitzung anzeigen und beenden

Sie können Ihr AWS Zugangsportal verwenden, um die Liste Ihrer aktiven Sitzungen einzusehen und bei Bedarf eine oder mehrere Sitzungen zu beenden.

Beenden Sie Ihre aktive Sitzung über Ihr AWS Zugangsportal

1. Melden Sie sich bei Ihrem AWS Zugangsportal an. Weitere Informationen finden Sie unter Melden Sie sich beim AWS Zugangsportal an.
2. Wählen Sie oben rechts auf der Seite Sicherheit aus.
3. Auf der Seite Sicherheit gibt die Zahl in Klammern neben Aktive Sitzungen an, wie viele aktive Sitzungen Sie haben. Aktivieren Sie das Kontrollkästchen neben jeder Sitzung, die Sie beenden möchten, und wählen Sie dann Sitzungen beenden aus.

   > **Tip**
   >
   > Bei Benutzerhintergrundsitzungen können Sie anhand des Amazon-Ressourcennamens (ARN) des Jobs, der die Sitzung verwendet, nach Sitzungen suchen. Wählen Sie in der Liste Sitzungstyp die Option Benutzerhintergrundsitzungen aus, und geben Sie dann den Job-ARN in das Suchfeld ein.

   Sie können nur aktive Sitzungen beenden, die geladen sind. Wenn Sie viele Sitzungen haben, wählen Sie Weitere aktive Sitzungen laden, um weitere Sitzungen anzuzeigen.
4. Aktivieren Sie das Kontrollkästchen neben jeder Sitzung, die Sie beenden möchten, und wählen Sie dann Sitzungen beenden aus.
5. Es wird ein Dialogfeld angezeigt, das bestätigt, dass Sie aktive Sitzungen beenden. Überprüfen Sie die Informationen, und wenn Sie fortfahren möchten, geben Sie den Text ein`confirm`, und wählen Sie dann Sitzungen beenden aus.
6. Sie kehren zu Ihrer Liste der aktiven Sitzungen zurück. Eine grüne Benachrichtigung zeigt an, dass die ausgewählten Sitzungen erfolgreich beendet wurden.

Resilienzdesign und regionales Verhalten

Der IAM Identity Center-Service wird vollständig verwaltet und nutzt hochverfügbare und langlebige AWS Dienste wie Amazon S3 und Amazon EC2. Um die Verfügbarkeit im Falle einer Störung der Availability Zone sicherzustellen, arbeitet IAM Identity Center in mehreren Verfügbarkeitszonen.

Sie aktivieren IAM Identity Center in Ihrem AWS Organizations Verwaltungskonto. Dies ist erforderlich, damit IAM Identity Center Rollen für all Ihre Benutzer bereitstellen, deren Bereitstellung aufheben und aktualisieren kann. AWS-Konten Wenn Sie IAM Identity Center aktivieren, wird es auf dem aktuell ausgewählten System AWS-Region bereitgestellt. Wenn Sie die Bereitstellung in einer bestimmten Region durchführen möchten AWS-Region, ändern Sie die Regionsauswahl, bevor Sie IAM Identity Center aktivieren.

> **Note**
>
> IAM Identity Center kontrolliert den Zugriff auf seine Berechtigungssätze und Anwendungen nur von seiner Hauptregion aus. Wir empfehlen, dass Sie die Risiken berücksichtigen, die mit der Zugriffskontrolle verbunden sind, wenn IAM Identity Center in einer einzigen Region betrieben wird.

IAM Identity Center bestimmt zwar, dass der Zugriff von der Region aus erfolgt, in der Sie den Service aktivieren, AWS-Konten gilt aber global. Das bedeutet, dass Benutzer, nachdem sie sich bei IAM Identity Center angemeldet haben, in jeder Region operieren können, wenn sie AWS-Konten über IAM Identity Center darauf zugreifen. Die meisten AWS verwalteten Anwendungen wie Amazon SageMaker AI müssen jedoch in derselben Region wie IAM Identity Center installiert sein, damit Benutzer sich authentifizieren und Zugriff auf diese Anwendungen zuweisen können. Informationen zu regionalen Einschränkungen bei der Verwendung einer Anwendung mit IAM Identity Center finden Sie in der Dokumentation zur 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 wurde.

Wir raten davon ab, dies Kontoinstanzen von IAM Identity Center als Mittel zur Implementierung von Resilienz zu verwenden, da dadurch ein zweiter, isolierter Kontrollpunkt entsteht, der nicht mit der Instanz Ihrer Organisation verbunden ist.

Auf Verfügbarkeit ausgelegt

Die folgende Tabelle zeigt die Verfügbarkeit, auf die IAM Identity Center ausgelegt ist. Diese Werte stellen kein Service Level Agreement oder eine Garantie dar, sondern geben vielmehr Aufschluss über die Designziele. Die Prozentsätze der Verfügbarkeit beziehen sich auf den Zugriff auf Daten oder Funktionen und nicht auf die Haltbarkeit (z. B. die langfristige Aufbewahrung von Daten).

Servicekomponente	Verfügbarkeitsdesignziel
Datenebene (einschließlich Anmeldung)	99.95%
Steuerebene	99.90%

Richten Sie den Notfallzugriff auf das ein AWS-Managementkonsole

IAM Identity Center basiert auf einer hochverfügbaren AWS Infrastruktur und verwendet eine Availability Zone-Architektur, um einzelne Fehlerquellen zu eliminieren. Für einen zusätzlichen Schutz im unwahrscheinlichen Fall eines IAM Identity Center oder einer AWS-Region Unterbrechung empfehlen wir Ihnen, eine Konfiguration einzurichten, die Sie für den temporären Zugriff auf das verwenden können. AWS-Managementkonsole

AWS ermöglicht Ihnen:

- Connect Ihren Drittanbieter-IdP mit dem IAM Identity Center.
- Connect Ihren Drittanbieter-IdP mit einer Einzelperson, AWS-Konten indem Sie einen SAML 2.0-basierten Verbund verwenden.

Wenn Sie IAM Identity Center verwenden, können Sie diese Funktionen verwenden, um die in den folgenden Abschnitten beschriebene Notfallzugriffskonfiguration zu erstellen. Diese Konfiguration ermöglicht es Ihnen, IAM Identity Center als Zugriffsmechanismus zu AWS-Konto verwenden. Wenn das IAM Identity Center unterbrochen wird, können sich Ihre Benutzer für den Notfallbetrieb AWS-Managementkonsole über einen direkten Verbund 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, die IAM-Datenebene und Ihr externer Identitätsanbieter (IdP) jedoch verfügbar sind.

> **Important**
>
> Wir empfehlen, dass Sie diese Konfiguration bereitstellen, bevor es zu einer Unterbrechung kommt, da Sie die Konfiguration nicht erstellen können, wenn Ihr Zugriff auf die Erstellung der erforderlichen IAM-Rollen ebenfalls unterbrochen ist. Testen Sie diese Konfiguration außerdem regelmäßig, um sicherzustellen, dass Ihr Team weiß, was zu tun ist, wenn IAM Identity Center unterbrochen wird.

Themen

Zusammenfassung der Konfiguration des Notfallzugriffs

Um den Notfallzugriff zu konfigurieren, müssen Sie die folgenden Aufgaben ausführen:

1. Erstellen Sie in Ihrer Organisation ein Notfallkonto für den Betrieb von Notfällen AWS Organizations. Dieses Konto wird zu Ihrem Notfallkonto.
2. Connect Sie Ihren IdP mithilfe eines SAML 2.0-basierten Verbunds mit dem Notfalleinsatzkonto.
3. Erstellen Sie im Notfallbetriebskonto eine Rolle für den Verbund von externen Identitätsanbietern. Erstellen Sie außerdem in jedem Ihrer Workload-Konten eine Notfalleinsatzrolle mit den erforderlichen Berechtigungen.
4. Delegieren Sie den Zugriff auf Ihre Workload-Konten für die IAM-Rolle, die Sie im Notfallbetriebskonto erstellt haben. Um den Zugriff auf Ihr Notfalleinsatzkonto zu autorisieren, erstellen Sie in Ihrem IdP eine Notfalleinsatzgruppe ohne Mitglieder.

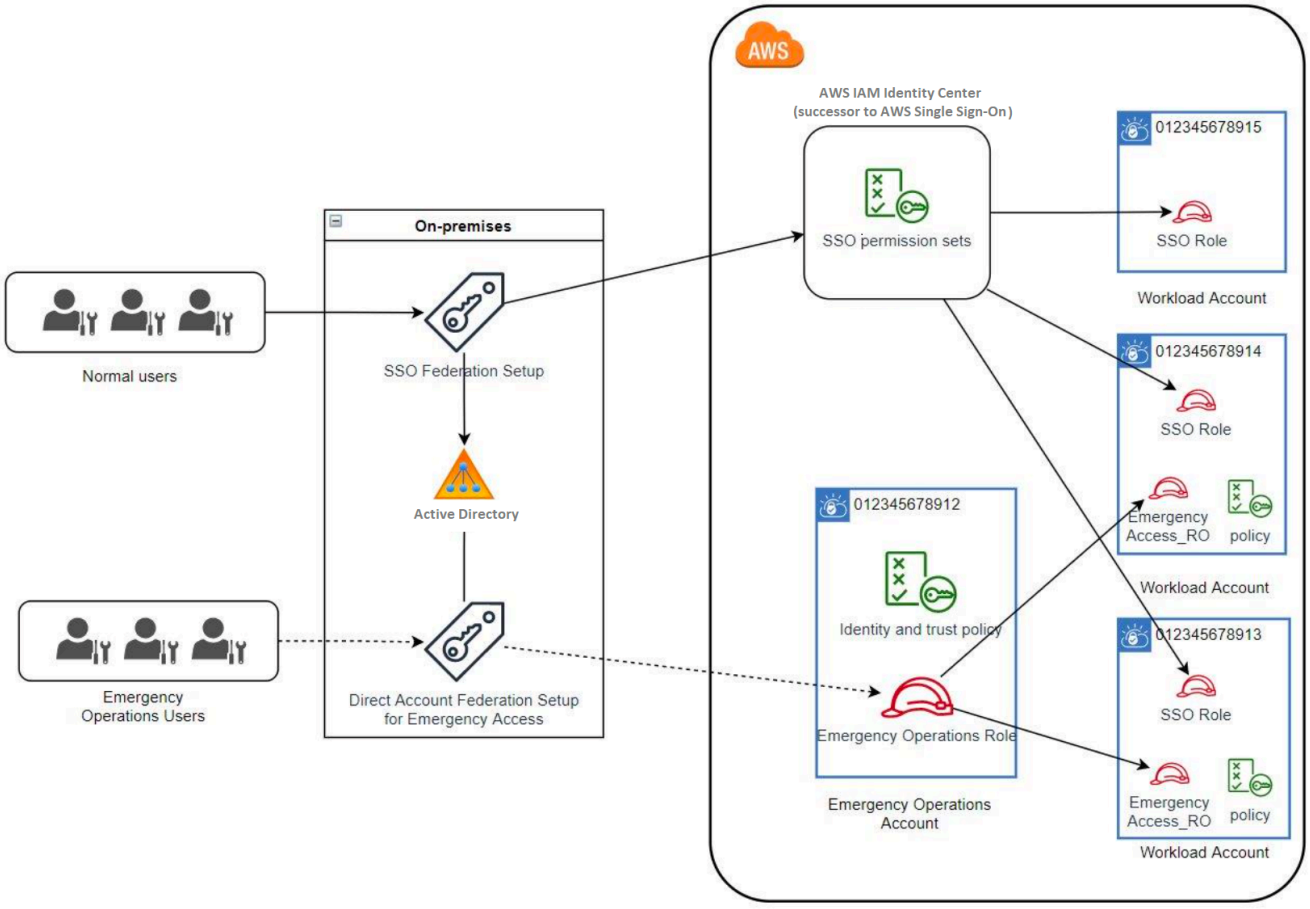
5. Ermöglichen Sie der Notfalleinsatzgruppe in Ihrem IdP die Verwendung der Notfalleinsatzrolle, indem Sie in Ihrem IdP eine Regel erstellen, die den SAML 2.0-Verbundzugriff auf die ermöglicht. AWS-Managementkonsole

Während des normalen Betriebs hat niemand Zugriff auf das Notfalleinsatzkonto, da die Notfalleinsatzgruppe in Ihrem IdP keine Mitglieder hat. Im Falle einer IAM Identity Center-Störung verwenden Sie Ihren IdP, um vertrauenswürdige Benutzer zur Notfalleinsatzgruppe in Ihrem IdP hinzuzufügen. Diese Benutzer können sich dann bei Ihrem IdP anmelden, zu dem AWS-Managementkonsole navigieren und die Rolle Notfallbetrieb im Notfalleinsatzkonto übernehmen. Von dort aus können diese Benutzer die Rolle für den Notfallzugriff in Ihren Workload-Konten übernehmen, wo sie Betriebsarbeiten ausführen müssen.

Wie gestalten Sie Ihre kritischen Operations-Rollen

Mit diesem Design konfigurieren Sie eine einzige Lösung, AWS-Konto in der Sie sich über IAM zusammenschließen, sodass Benutzer wichtige Betriebsrollen übernehmen können. Die Rollen für kritische Operationen verfügen über eine Vertrauensrichtlinie, die es Benutzern ermöglicht, eine entsprechende Rolle in Ihren Workload-Konten einzunehmen. Die Rollen in den Workload-Konten stellen die Berechtigungen bereit, die Benutzer benötigen, um wichtige Aufgaben auszuführen.

Das folgende Diagramm bietet einen Überblick über den Entwurf.



Wie planen Sie Ihr Zugriffsmodell

Bevor Sie den Notfallzugriff konfigurieren, erstellen Sie einen Plan, wie das Zugriffsmodell funktionieren soll. Gehen Sie wie folgt vor, um diesen Plan zu erstellen.

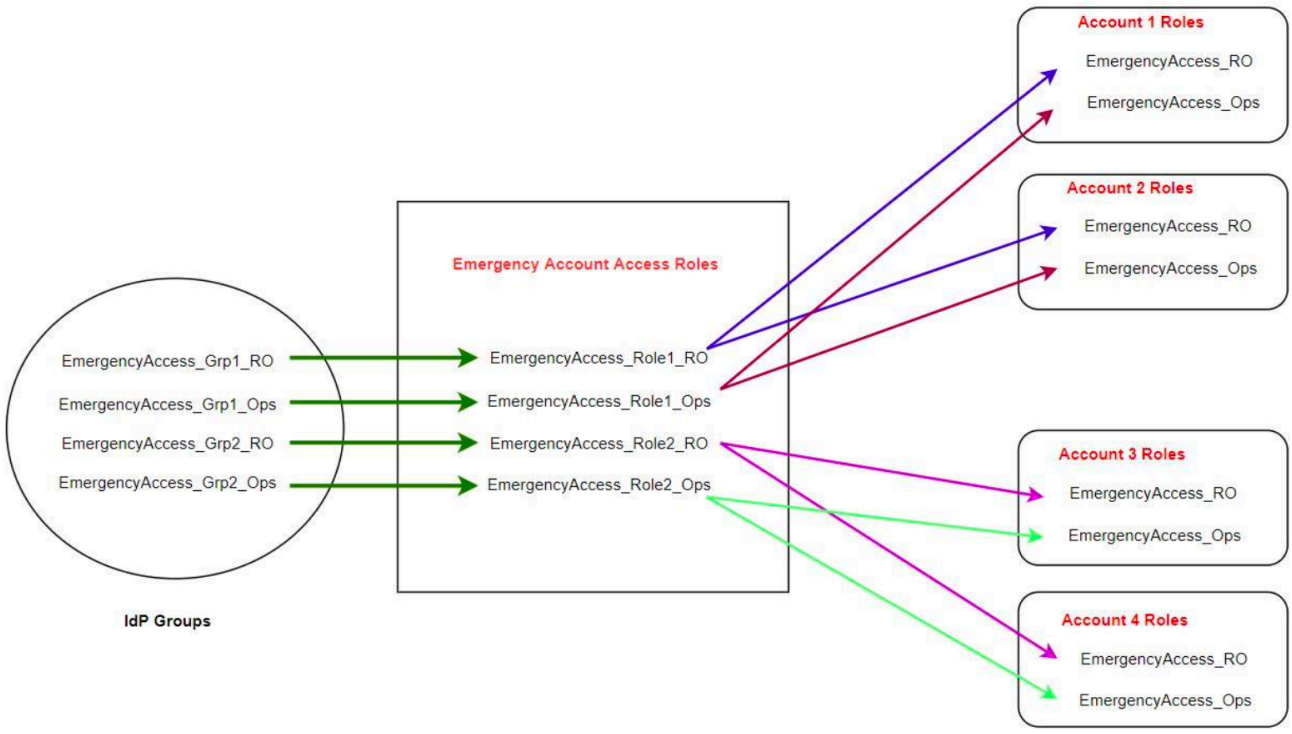
1. Identifizieren Sie die AWS-Konten Bereiche, in denen der Notfalldienst während einer Unterbrechung des IAM Identity Center unbedingt erforderlich ist. Beispielsweise sind Ihre Produktionskonten wahrscheinlich unverzichtbar, Ihre Entwicklungs- und Testkonten jedoch möglicherweise nicht.
2. Identifizieren Sie für diese Sammlung von Konten die spezifischen kritischen Rollen, die Sie in Ihren Konten benötigen. Definieren Sie bei all diesen Konten einheitlich, was die Rollen leisten können. Dies vereinfacht die Arbeit in Ihrem Notfallzugriffskonto, in dem Sie kontenübergreifende Rollen erstellen. Wir empfehlen, dass Sie in diesen Konten mit zwei unterschiedlichen Rollen beginnen: Read Only (RO) und Operations (Ops). Bei Bedarf können Sie weitere Rollen erstellen

und diese Rollen in Ihrem Setup einer eindeutigeren Gruppe von Benutzern mit Notfallzugriff 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 in Ihrem IdP Regeln, die Ansprüche generieren, die auflisten, auf welche Rollen die Gruppe zugreifen kann. Diese Gruppen können dann Ihre Rollen „Nur Lesen“ oder „Operations“ im Notfallzugriffskonto übernehmen. Von diesen Rollen aus können sie die entsprechenden Rollen in Ihren Workload-Konten übernehmen.

Wie gestaltet man die Rollen-, Konto- und Gruppenzuordnungen für Notfälle

Das folgende Diagramm zeigt, wie Sie Ihre Notfallzugriffsgruppen den Rollen in Ihrem Notfallzugriffskonto zuordnen. Das Diagramm zeigt auch die kontenübergreifenden Rollenvertrauensbeziehungen, die es Kontorollen mit Notfallzugriff ermöglichen, auf die entsprechenden Rollen in Ihren Workload-Konten zuzugreifen. Wir empfehlen, bei der Gestaltung Ihres Notfallplans diese Zuordnungen als Ausgangspunkt zu verwenden.



So erstellen Sie Ihre Notfallzugriffskonfiguration

Verwenden Sie die folgende Zuordnungstabelle, um Ihre Notfallzugriffskonfiguration zu erstellen. Diese Tabelle zeigt einen Plan, der zwei Rollen in den Workload-Konten umfasst: Read Only (RO) und Operations (Ops) mit den entsprechenden Vertrauens- und Berechtigungsrichtlinien. Die Vertrauensrichtlinien ermöglichen es den Notfallzugriffskontorollen, auf die einzelnen Workload-Kontorollen zuzugreifen. Die einzelnen Workload-Kontorollen verfügen auch über Berechtigungsrichtlinien für die Aufgaben, die die Rolle im Konto ausführen kann. Bei den Berechtigungsrichtlinien kann AWS es sich um verwaltete Richtlinien oder um vom Kunden verwaltete Richtlinien handeln.

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
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 die Rolle „Ressource“ im Konto

In diesem Zuordnungsplan enthält das Notfallzugriffskonto zwei Rollen mit Schreibschutz und zwei Rollen für den Betrieb. Diese Rollen vertrauen darauf, dass Ihr IdP Ihre ausgewählten Gruppen authentifiziert und autorisiert, auf die Rollen zuzugreifen, indem er die Namen der Rollen in Assertionen weitergibt. In Workload Account 1 und Account 2 gibt es entsprechende Nur-Lese-Rollen und Operations-Rollen. Für Workload-Konto 1 vertraut die `EmergencyAccess_R0` Rolle der Rolle, die sich im `EmergencyAccess_Role1_R0` Notfallzugriffskonto befindet. In der Tabelle sind ähnliche Vertrauensmuster zwischen den Rollen „Schreibgeschützt“ und „Betrieb“ des Workload-Kontos und den entsprechenden Rollen für den Notfallzugriff angegeben.

Aufgaben zur Notfallvorbereitung

Um Ihre Notfallzugriffskonfiguration vorzubereiten, empfehlen wir Ihnen, die folgenden Aufgaben durchzuführen, 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 der Veranstaltung 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 für jedes der Workload-Konten.
5. Erstellen Sie temporäre Betriebsgruppen in Ihrem IdP. Die Gruppennamen hängen von den Namen der temporären Betriebsrollen ab.
6. Testen Sie den direkten IAM-Verbund.
7. Deaktivieren Sie die IdP-Verbundanwendung in Ihrem IdP, um eine regelmäßige Nutzung zu verhindern.

Failover-Prozess für Notfälle

Wenn eine IAM Identity Center-Instanz nicht verfügbar ist und Sie feststellen, dass Sie Notfallzugriff auf die AWS Management Console gewähren müssen, empfehlen wir den folgenden Failover-Prozess.

1. Der IdP-Administrator aktiviert die direkte IAM-Verbundanwendung in Ihrem IdP.

2. Benutzer beantragen Zugriff auf die temporäre Betriebsgruppe über Ihren bestehenden Mechanismus, z. B. eine E-Mail-Anfrage, einen Slack-Channel oder eine andere Form der Kommunikation.
3. Benutzer, die Sie zu Ihren Notfallzugriffsgruppen hinzufügen, melden sich beim IdP an, wählen das Notfallzugriffskonto aus, und Benutzer wählen eine Rolle aus, die im Notfallzugriffskonto verwendet werden soll. Von diesen Rollen aus können sie Rollen in entsprechenden Workload-Konten übernehmen, denen kontenübergreifendes Vertrauen mit der Notfallkontorolle gilt.

Kehren Sie zum normalen Betrieb zurück

Überprüfen Sie das AWS Health Dashboard, um zu überprüfen, ob der Zustand des IAM Identity Center-Dienstes wiederhergestellt ist. Gehen Sie wie folgt vor, um zum normalen Betrieb zurückzukehren.

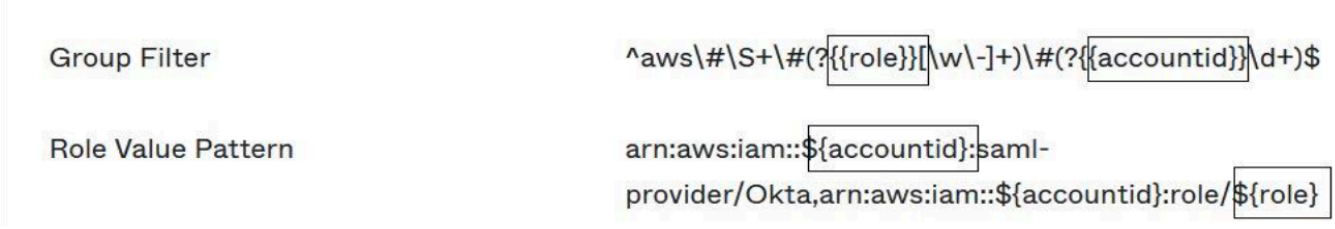
1. Wenn das Statussymbol für den IAM Identity Center-Dienst anzeigt, dass der Dienst fehlerfrei ist, melden Sie sich bei IAM Identity Center an.
2. Wenn Sie sich erfolgreich beim IAM Identity Center anmelden können, teilen Sie den Benutzern mit Notfallzugriff mit, dass IAM Identity Center verfügbar ist. Weisen Sie diese Benutzer an, sich abzumelden und sich über das AWS Zugriffsportal wieder bei IAM Identity Center anzumelden.
3. Nachdem sich alle Benutzer mit Notfallzugriff abgemeldet haben, deaktivieren Sie im IdP die IdP-Verbundanwendung. Wir empfehlen, dass Sie diese Aufgabe außerhalb der Geschäftszeiten ausführen.
4. Entfernen Sie alle Benutzer aus der Notfallzugriffsgruppe im IdP.

Ihre Rolleninfrastruktur für den Notfallzugriff bleibt als Backup-Zugriffsplan bestehen, ist aber jetzt deaktiviert.

Einmalige Einrichtung einer direkten IAM-Verbundanwendung in Okta

1. Melden Sie sich als Benutzer mit Administratorrechten bei Ihrem Okta Konto an.
2. Wählen Sie in der Okta Admin-Konsole unter Anwendungen die Option Anwendungen aus.
3. Wählen Sie „App-Katalog durchsuchen“. Suchen Sie nach AWS Account Federation und wählen Sie es aus. Wählen Sie dann Integration hinzufügen.
4. Richten Sie einen direkten IAM-Verbund 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 die Option SAML 2.0 aus und geben Sie die Einstellungen für Gruppenfilter und Rollenwertmuster ein. Der Name der Gruppe für das Benutzerverzeichnis hängt vom Filter ab, den Sie konfigurieren.



   In der Abbildung oben bezieht sich die `role` Variable auf die Rolle „Notfallbetrieb“ in Ihrem Notfallzugriffskonto. Wenn Sie beispielsweise die `EmergencyAccess_Role1_R0` Rolle (wie in der Zuordnungstabelle beschrieben) in erstellen und Ihre Gruppenfiltereinstellung so konfiguriert ist AWS-Konto `123456789012`, wie in der Abbildung oben gezeigt, sollte Ihr Gruppenname lauten`aws#EmergencyAccess_Role1_R0#123456789012`.

6. Erstellen Sie in Ihrem Verzeichnis (z. B. Ihrem Verzeichnis in Active Directory) die Notfallzugriffsgruppe und geben Sie einen Namen für das Verzeichnis an (z. B.`aws#EmergencyAccess_Role1_R0#123456789012`). Weisen Sie Ihre Benutzer dieser Gruppe zu, indem Sie Ihren vorhandenen Bereitstellungsmechanismus verwenden.

7. Konfigurieren Sie im Notfallzugriffskonto eine benutzerdefinierte Vertrauensrichtlinie, die die erforderlichen Berechtigungen bereitstellt, damit die Notfallzugriffsrolle während einer Störung übernommen werden kann. Im Folgenden finden Sie eine Beispielanweisung für eine benutzerdefinierte Vertrauensrichtlinie, die der `EmergencyAccess_Role1_R0` Rolle zugeordnet ist. Eine Veranschaulichung finden Sie in der Abbildung unten unter dem NotfallkontoWie gestaltet man die Rollen-, Konto- und Gruppenzuordnungen für Notfälle.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
      {
         "Effect":"Allow",
         "Principal":{
            "Federated":"arn:aws:iam::123456789012:saml-provider/Okta"
         },
         "Action":[
            "sts:AssumeRoleWithSAML",
```

```
            "sts:TagSession"
         ],
         "Condition":{
            "StringEquals":{
               "SAML:aud": "https://signin.aws.amazon.com/saml"
            }
         }
      },
      {
         "Effect":"Allow",
         "Principal":{
         "Federated":"arn:aws:iam::123456789012:saml-provider/Okta"
         },
         "Action":"sts:SetSourceIdentity"
       }
   ]
}
```

8. Im Folgenden finden Sie eine Beispielanweisung für eine Berechtigungsrichtlinie, die der `EmergencyAccess_Role1_R0` Rolle zugeordnet ist. Eine Veranschaulichung finden Sie in der Abbildung unten unter dem NotfallkontoWie gestaltet man die Rollen-, Konto- und Gruppenzuordnungen für Notfälle.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": [
                "arn:aws:iam::111122223333:role/EmergencyAccess_RO",
                "arn:aws:iam::444455556666:role/EmergencyAccess_RO"
            ]
        }
    ]
}
```

9. Konfigurieren Sie für die Workload-Konten eine benutzerdefinierte Vertrauensrichtlinie. Im Folgenden finden Sie ein Beispiel für eine Vertrauensrichtlinie, die der `EmergencyAccess_R0`

Rolle zugeordnet ist. In diesem Beispiel `123456789012` ist Konto das Notfallzugriffskonto. Eine Veranschaulichung finden Sie in der Abbildung unten unter Workload-KontoWie gestaltet man die Rollen-, Konto- und Gruppenzuordnungen für Notfälle.

JSON

```
{
    "Version":"2012-10-17",
    "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "AWS":"arn:aws:iam::123456789012:root"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

> **Note**
>
> In den IdPs meisten Fällen können Sie eine Anwendungsintegration so lange deaktivieren, bis sie benötigt wird. Wir empfehlen Ihnen, die direkte IAM-Verbundanwendung in Ihrem IdP so lange deaktiviert zu lassen, bis sie für den Notfallzugriff benötigt wird.

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.

Topics

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.

> **Note**
>
> Wenn Ihre IAM Identity Center-Instanz mit einem vom Kunden verwalteten KMS-Schlüssel konfiguriert ist, benötigen Ihre IAM Identity Center-Administratoren und andere Akteure, die Zugriff auf den KMS-Schlüssel benötigen, zusätzliche Berechtigungen. Weitere Informationen finden Sie unter Implementierung von vom Kunden verwalteten KMS-Schlüsseln in AWS IAM Identity Center.

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
- Beispiel für eine ressourcenbasierte Richtlinie für IAM Identity Center (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
- Verwaltung 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.

Verwaltung 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.

JSON

```
{
   "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 (siheRessourcen 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"), ist der Zugriff 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 allgemeine 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 Rollen zuordnen. and/or 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
- Beispiel 2: Erlauben Sie einem Benutzer, seine Berechtigungen AWS-Konten in IAM Identity Center zu verwalten
- Beispiel 3: Erlauben Sie einem Benutzer, Anwendungen in IAM Identity Center zu verwalten
- Beispiel 4: Erlauben Sie einem Benutzer, Benutzer und Gruppen in Ihrem Identity Center-Verzeichnis zu verwalten

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.

JSON

```
{
    "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:ListDelegatedAdministrators",
                "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

JSON

```
{
    "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": "AccessToSSOProvisionedRoles"` 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.

JSON

```
{
    "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.

JSON

```
{
    "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.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:DescribeAccountAssignmentCreationStatus",
                "sso:DescribeAccountAssignmentDeletionStatus",
                "sso:DescribePermissionSet",
                "sso:DescribePermissionSetProvisioningStatus",
                "sso:DescribeRegisteredRegions",
                "sso:GetApplicationInstance",
                "sso:GetApplicationTemplate",
                "sso:GetInlinePolicyForPermissionSet",
                "sso:GetManagedApplicationInstance",
                "sso:GetMfaDeviceManagementForDirectory",
                "sso:GetPermissionSet",
                "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": "*"
        }
    ]
}
```

Beispiel für eine ressourcenbasierte Richtlinie für IAM Identity Center (IAM Identity Center)

Jede Anwendung, die mit IAM Identity Center funktioniert und OAuth 2.0 verwendet, erfordert eine ressourcenbasierte Richtlinie. Die Anwendung kann vom Kunden verwaltet oder verwaltet werden. AWS Die erforderliche ressourcenbasierte Richtlinie, die als Anwendungsrichtlinie (oder ActorPolicyin der APIs) bezeichnet wird, definiert, welche IAM-Prinzipale berechtigt sind, API-Aktionen für die IAM-Authentifizierungsmethode aufzurufen, z. B. `CreateTokenWithIAM` Die IAM-Authentifizierungsmethode ermöglicht es einem IAM-Prinzipal, z. B. einer IAM-Rolle oder einem AWS Dienst, sich beim IAM Identity Center OIDC-Dienst zu authentifizieren, indem er IAM-Anmeldeinformationen vorlegt, um Zugriffstoken unter /token? anzufordern oder zu verwalten Endpunkt aws_iam=t.

Die Anwendungsrichtlinie regelt die Vorgänge zur Ausgabe von Token (). `CreateTokenWithIAM` Die Richtlinie regelt auch Aktionen, für die nur Berechtigungen erforderlich sind und nur von AWS verwalteten Anwendungen zur Validierung von Token () und zum Widerruf von Token (`IntrospectTokenWithIAM`) verwendet werden. `RevokeTokenWithIAM` Für eine vom Kunden verwaltete Anwendung konfigurieren Sie diese Richtlinie, indem Sie angeben, welche IAM-Principals

aufrufen dürfen. `CreateTokenWithIAM` Wenn ein autorisierter Principal diese API-Aktion aufruft, erhält der Principal Zugriffs- und Aktualisierungstoken für die Anwendung.

Wenn Sie die IAM Identity Center-Konsole verwenden, um eine vom Kunden verwaltete Anwendung für die Weitergabe vertrauenswürdiger Identitäten einzurichten, finden Sie in Schritt 4 unter Kundenverwaltete OAuth 2.0-Anwendungen einrichten Informationen zur Konfiguration der Anwendungsrichtlinie. Ein Beispiel für eine Richtlinie finden Sie weiter Beispielrichtlinie: Erlaubt einer IAM-Rolle, Zugriffs- und Aktualisierungstoken zu erstellen unten in diesem Thema.

Anforderungen an die Richtlinie

Die Richtlinie muss die folgenden Anforderungen erfüllen:

- Die Richtlinie muss ein `Version` Element enthalten, das auf „2012-10-17“ gesetzt ist.
- Die Richtlinie muss mindestens ein Element enthalten. `Statement`
- Jede Richtlinie `Statement` muss die folgenden Elemente enthalten: `Effect`,`Principal`,`Action`, und`Resource`.

Richtlinienelemente

Die Richtlinie muss die folgenden Elemente enthalten:

Version

Gibt die Version des Richtliniendokuments an. Wir empfehlen, die Version auf `2012-10-17` (neueste Version) einzustellen.

Statement

Enthält die Richtlinie`Statements`. Die Richtlinie muss mindestens eine enthalten`Statement`.

Jede Richtlinie `Statement` besteht aus den folgenden Elementen.

Auswirkung

(Erforderlich) Gibt an, ob die Berechtigungen in der Richtlinienanweisung zugelassen oder verweigert werden. Gültige Werte sind `Allow` oder `Deny`.

Auftraggeber

(Erforderlich) Der Prinzipal ist die Identität, die die in der Richtlinienanweisung angegebenen Berechtigungen erhält. Sie können IAM-Rollen oder AWS Dienstprinzipale angeben.

Action

(Erforderlich) Die IAM Identity Center OIDC-Dienst-API-Operationen, die zugelassen oder verweigert werden sollen. Zu den gültigen Aktionen gehören:

- `sso-oauth:CreateTokenWithIAM`: Diese Aktion, die dem `CreateTokenWithIAM`API-Vorgang entspricht, gewährt die Berechtigung zum Erstellen und Zurückgeben von Zugriffs- und Aktualisierungstoken für autorisierte Client-Anwendungen, die mit einer beliebigen IAM-Entität authentifiziert wurden, z. B. einer AWS Servicerolle oder einem Benutzer. Diese Token können definierte Bereiche enthalten, die Berechtigungen wie oder spezifizieren. `read:profile` `write:data`
- `sso-oauth:IntrospectTokenWithIAM`[nur Berechtigung]: Erteilt die Berechtigung zum Überprüfen und Abrufen von Informationen über Active OAuth 2.0-Zugriffstoken und Aktualisierungstoken, einschließlich der zugehörigen Bereiche und Berechtigungen. Diese Berechtigung wird nur von AWS verwalteten Anwendungen verwendet und ist nicht in der IAM Identity Center OIDC API-Referenz dokumentiert.
- `RevokeTokenWithIAM` [nur Erlaubnis]: Erteilt die Erlaubnis, OAuth 2.0-Zugriffstoken zu widerrufen und Token zu aktualisieren, wodurch sie vor ihrem normalen Ablauf ungültig werden. Diese Berechtigung wird nur von AWS verwalteten Anwendungen verwendet und ist nicht in der IAM Identity Center OIDC API-Referenz dokumentiert.

Ressource

(Erforderlich) In dieser Richtlinie lautet der Wert des `Resource` Elements`"*"`, was „diese Anwendung“ bedeutet.

Weitere Informationen zur AWS Richtliniensyntax finden Sie unter AWS IAM-Richtlinienreferenz im IAM-Benutzerhandbuch.

Beispielrichtlinie: Erlaubt einer IAM-Rolle, Zugriffs- und Aktualisierungstoken zu erstellen

Die folgende Berechtigungsrichtlinie gewährt einer IAM-Rolle`ExampleAppClientRole`, die von einem Workload übernommen wurde, Berechtigungen zum Erstellen und Zurückgeben von Zugriffs- und Aktualisierungstoken.

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

```
    "Statement": [
        {
            "Sid": "AllowRoleToCreateTokens",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/ExampleAppClientRole"
            },
            "Action": "sso-oauth:CreateTokenWithIAM",
            "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: AWSSSOMaster AccountAdministrator

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 für alle 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.

Diese Richtlinie umfasst auch die erforderlichen AWS Key Management Service Berechtigungen für IAM Identity Center-Instanzen, die vom Kunden verwaltete Schlüssel zur Verschlüsselung verwenden.

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 Konfigurieren Sie den Zugriff 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: AWSSSOMember AccountAdministrator.

- `AWSSSOManageDelegatedAdministrator`— Ermöglicht IAM Identity Center die Registrierung und Abmeldung eines delegierten Administrators für Ihre Organisation.
- `AllowKMSKeyUseViaService`und `AllowKMSKeyDiscovery` — Ermöglicht AWS Key Management Service Operationen für vom Kunden verwaltete Schlüssel, die von IAM Identity Center-Instanzen verwendet werden.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AWSSSOMasterAccountAdministratorReferenz für AWS verwaltete 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 und. `iam:CreateServiceLinkedRole` `iam:PassRole`

AWS verwaltete Richtlinie: AWSSSOMember AccountAdministrator

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.

Diese Richtlinie umfasst auch die erforderlichen AWS Key Management Service Berechtigungen für IAM Identity Center-Instanzen, die vom Kunden verwaltete Schlüssel zur Verschlüsselung verwenden.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter Referenz AWSSSOMemberAccountAdministratorzu AWS verwalteten 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 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 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: AWSSSODirectory Administrator

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. Diese Richtlinie umfasst auch die erforderlichen AWS Key Management Service Berechtigungen für IAM Identity Center-Instanzen, die vom Kunden verwaltete Schlüssel zur Verschlüsselung verwenden.

Diese Richtlinie umfasst die folgenden Berechtigungen:

- IAM Identity Center Directory — Vollständiger Administratorzugriff auf IAM Identity Center-Verzeichnisoperationen.
- Identity Store — Vollständiger Administratorzugriff auf Identity Store-Operationen und Authentifizierung.
- IAM Identity Center — Berechtigung zum Auflisten von Verzeichniszuordnungen.
- AWS Key Management Service- Berechtigungen zum Entschlüsseln, Beschreiben und Generieren von Datenschlüsseln für vom Kunden verwaltete Schlüssel, die von IAM Identity Center-Instanzen verwendet werden.

Die Berechtigungen für diese Richtlinie finden Sie unter AWSSSODirectoryAdministrator in der Referenz für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: AWSSSORead Nur

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.

Diese Richtlinie umfasst auch die erforderlichen AWS Key Management Service Berechtigungen für IAM Identity Center-Instanzen, die vom Kunden verwaltete Schlüssel zur Verschlüsselung verwenden.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AWSSSOReadNur in der Referenz für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: AWSSSODirectory ReadOnly

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.

Diese Richtlinie umfasst auch die erforderlichen AWS Key Management Service Berechtigungen für IAM Identity Center-Instanzen, die vom Kunden verwaltete Schlüssel zur Verschlüsselung verwenden.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter Referenz AWSSSODirectoryReadOnlyzu AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: AWSIdentity SyncFullAccess

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: AWSIdentity SyncReadOnlyAccess

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: AWSSSOService RolePolicy

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: AWSIAMIdentity CenterAllowListForIdentityContext

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.

AWS verwaltete Richtlinie: AWSIdentity CenterExternalManagementPolicy

Sie können die `AWSIdentityCenterExternalManagementPolicy`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie bietet Zugriff auf die Verwaltung von IAM Identity Center-Benutzern von einem externen Anbieter aus.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AWSIdentityCenterExternalManagementPolicyReferenz für AWS verwaltete 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.

Änderungen	Beschreibung	Date
AWSIdentityCenterExternalManagementPolicy	Die verwaltete Richtlinie wurde aktualisiert, um den ARN für den Bereitstellungsmandanten zu ändern.	5. Dezember 2025
AWSIdentityCenterExternalManagementPolicy	Diese Richtlinie bietet Zugriff auf die Verwaltung von IAM Identity Center-Benutzern von einem externen Anbieter aus.	21. November 2025
AWSSSOMasterAccountAdministrator, AWSSSOMemberAccountAdministrator, AWSSSOReadNur, AWSSSODirectoryAdministrator, AWSSSODirectoryReadOnly	Die verwalteten Richtlinien wurden aktualisiert und enthalten AWS KMS nun auch die erforderlichen Berechtigungen für IAM Identity Center-Instanzen, die vom Kunden verwaltete Schlüssel zur Verschlüsselung verwenden.	17. September 2025
AWSSSOServiceRolePolicy	Diese Richtlinie umfasst jetzt auch Anrufberechtigunge `nidentity-sync:DeleteSyncProfile` .	11. Februar 2025
AWSIAMIdentityCenterAllowListForIdentityContext	Diese Richtlinie umfasst jetzt die `qapps:ListQAppSessionData` und `qapps:ExportQAppSessionData` Aktionen zur Unterstützung	2. Oktober 2024

Änderungen	Beschreibung	Date
	von Konsolensitzungen mit verbesserter Identität für AWS verwaltete Anwendungen, die diese Sitzungen unterstützen.	
AWSSSOMasterAccountAdministrator	IAM Identity Center hat eine neue Aktion hinzugefügt, mit der Sie DeleteSyncProfile Berechtigungen erteilen können, damit Sie diese Richtlinie zum Löschen von Synchronisationsprofilen verwenden können. Diese Aktion ist mit der DeleteInstance API verknüpft.	26. September 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Diese Richtlinie umfasst jetzt die `s3:ListCallerAccessGrants` Aktion zur Unterstützung von Konsolensitzungen mit verbesserter Identität für AWS verwaltete Anwendungen, die diese Sitzungen unterstützen.	4. September 2024

Änderungen	Beschreibung	Date
AWSIAMIdentityCenterAllowListForIdentityContext	Diese Richtlinie umfasst jetzt die `es:ESHttpPut` Aktionen`aoss:APIAccessAll` ,,`es:ESHttpHead` ,, `es:ESHttpPost` `es:ESHttpGet` `es:ESHttpPatch` `es:ESHttpDelete` , und zur Unterstützung von Konsolensitzungen mit verbesserter Identität für AWS verwaltete Anwendungen, die diese Sitzungen unterstützen.	12. Juli 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Diese Richtlinie umfasst nun die`qapps:PredictQApp` ,,,`qapps:ImportDocument` ,`qapps:AssociateLibraryItemReview` , `qapps:DisassociateLibraryItemReview` `qapps:GetQAppSession` `qapps:UpdateQAppSession` `qapps:GetQAppSessionMetadata` `qapps:UpdateQAppSessionMetadata` , und `qapps:TagResource` Aktionen zur Unterstützung von Konsolensitzungen mit verbesserter Identität für AWS verwaltete Anwendungen, die diese Sitzungen unterstützen.	27. Juni 2024

Änderungen	Beschreibung	Date
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

Änderungen	Beschreibung	Date
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:ImportDocumentToQApp` ,`qapps:ImportDocumentToQAppSession` ,`qapps:CreateLibraryItem` ,`qapps:GetLibraryItem` , `qapps:UpdateLibraryItem` `qapps:CreateLibraryItemReview` `qapps:ListLibraryItems` `qapps:CreateSubscriptionToken` `qapps:StartQAppSession` , und `qapps:StopQAppSession` Aktionen zur Unterstützung von	30. April 2024

Änderungen	Beschreibung	Date
	Konsolensitzungen mit verbesserter Identität für AWS verwaltete Anwendungen, die diese Sitzungen unterstützen.	
AWSSSOMasterAccountAdministrator	Diese Richtlinie umfasst jetzt die `signin:CreateTrustedIdentityPropagationApplicationForConsole` und `signin:ListTrustedIdentityPropagationApplicationsForConsole` Aktionen zur Unterstützung von Konsolensitzungen mit verbesserter Identität für AWS verwaltete Anwendungen, die diese Sitzungen unterstützen.	26. April 2024
AWSSSOMemberAccountAdministrator	Diese Richtlinie umfasst jetzt die `signin:CreateTrustedIdentityPropagationApplicationForConsole` und `signin:ListTrustedIdentityPropagationApplicationsForConsole` Aktionen zur Unterstützung von Konsolensitzungen mit verbesserter Identität für AWS verwaltete Anwendungen, die diese Sitzungen unterstützen.	26. April 2024

Änderungen	Beschreibung	Date
AWSSSOReadNur	Diese Richtlinie umfasst jetzt die `signin:ListTrustedIdentityPropagationApplicationsForConsole` Aktion zur Unterstützung von Konsolensitzungen mit verbesserter Identität für AWS verwaltete Anwendungen, die diese Sitzungen unterstützen.	26. April 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Diese Richtlinie umfasst jetzt die `qbusiness:PutFeedback` Aktion zur Unterstützung von Konsolensitzungen mit verbesserter Identität für AWS verwaltete Anwendungen, die diese Sitzungen unterstützen.	26. April 2024

Änderungen	Beschreibung	Date
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 von Konsolensitzungen mit verbesserter Identität für AWS verwaltete Anwendungen, die diese Sitzungen unterstützen.	24. April 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Diese Richtlinie umfasst jetzt die `sts:SetContext` Aktion zur Unterstützung von Konsolensitzungen mit verbesserter Identität für AWS verwaltete Anwendungen, die diese Sitzungen unterstützen.	19. April 2024

Änderungen	Beschreibung	Date
AWSIAMIdentityCenterAllowListForIdentityContext	Diese Richtlinie umfasst jetzt die `qbusiness:DeleteConversation` Aktionen `qbusiness:Chat` ,, `qbusiness:ChatSync` `qbusiness:ListConversations` `qbusiness:ListMessages` , und zur Unterstützung von Konsolensitzungen mit verbesserter Identität für AWS verwaltete Anwendungen, die diese Sitzungen unterstützen.	11. April 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Diese Richtlinie umfasst jetzt die Aktionen `s3:GetAccessGrantsInstanceForPrefix` und `s3:GetDataAccess` .	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

Änderungen	Beschreibung	Date
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

Änderungen	Beschreibung	Date
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 BerechtigungenAWSSSOManageDelegatedAdministrator , zu der auch Anrufberechtigungen `RegisterDelegatedAdministrator` und `DeregisterDelegatedAdministrator` gehören.	16. August 2022

Änderungen	Beschreibung	Date
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
AWSSSOReadNur	Diese Richtlinie umfasst jetzt neue ListDelegatedAdministrators_ Anrufberechtigungen AWS Organizations.	11. August 2022
AWSSSOServiceRolePolicy	Diese Richtlinie umfasst jetzt neue Anrufberechtigungen DeleteRolePermissionsBoundary und PutRolePermisionsBoundary .	14. Juli 2022

Änderungen	Beschreibung	Date
AWSSSOServiceRolePolicy	Diese Richtlinie umfasst jetzt neue Berechtigungen, die eingehende Anrufe ermöglichen `ListAWSServiceAccessForOrganization` and `ListDelegatedAdministrators` AWS Organizations.	11. Mai 2022
AWSSSOMasterAccountAdministrator AWSSSOMemberAccountAdministrator AWSSSOReadNur	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

Änderungen	Beschreibung	Date
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
AWSSSOReadNur	Diese Richtlinie gewährt nur Leseberechtigungen, 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 Grundlegendes zu serviceverknüpften Rollen in IAM Identity Center.

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 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 dienstgebundene AWSService RoleFor SSO-Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- IAM Identity Center (Dienstpräfix:) `sso`

Die Richtlinie für AWSSSOService RolePolicy dienstbezogene Rollenberechtigungen ermöglicht es IAM Identity Center, für Rollen im Pfad „/aws-reserved/sso.amazonaws.com/“ und mit dem Namenspräfix „SSO_“ Folgendes auszuführen: AWSReserved

- `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 AWSSSOService RolePolicy 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 AWSSSOService RolePolicy 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 AWSSSOService RolePolicy dienstbezogene Rollenberechtigungen ermöglicht es IAM Identity Center, Folgendes für alle IAM-Rollen durchzuführen (*):

- iam:listRoles

Die Richtlinie für AWSSSOService RolePolicy dienstbezogene Rollenberechtigungen ermöglicht es IAM Identity Center, auf „arn:aws:iam: :*:“ Folgendes auszuführen: role/aws-service-role/sso.amazonaws.com/AWSServiceRoleForSSO

- `iam:GetServiceLinkedRoleDeletionStatus`
- `iam:DeleteServiceLinkedRole`

Die Richtlinie für AWSSSOService RolePolicy dienstbezogene Rollenberechtigungen ermöglicht es IAM Identity Center, auf „arn:aws:identity-sync: *:*:profile/*“ Folgendes auszuführen:

- `identity-sync:DeleteSyncProfile`

Weitere Informationen zu Aktualisierungen der Richtlinie für Berechtigungen für dienstverknüpfte Rollen finden Sie unter. AWSSSOService RolePolicy IAM Identity Center aktualisiert AWS verwaltete Richtlinien

JSON

```
{
   "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":[
            "*"
         ]
      },
      {
         "Sid":"AllowDeleteSyncProfile",
         "Effect":"Allow",
         "Action":[
            "identity-sync:DeleteSyncProfile"
         ],
         "Resource":[
```

```
            "arn:aws:identity-sync:*:*:profile/*"
        ]
      }
   ]
}
```

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 dienstverknüpfte 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 AWSService RoleFor SSO-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 mit dem AWSService RoleFor SSO-Dienst verknüpfte Rolle nicht bearbeiten. 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 AWSService RoleFor SSO-Rolle nicht manuell löschen. 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 vom SSO verwendete IAM Identity Center-Ressourcen zu löschen AWSService RoleFor

1. Entfernen Sie den Benutzer- und Gruppenzugriff auf ein AWS-Kontofür alle Benutzer und Gruppen, die Zugriff auf die AWS-Konto haben.
2. Entfernen Sie die Berechtigungssätze im IAM Identity Centerdie 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 mit dem AWSService RoleFor SSO-Dienst verknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Leitfaden.

IAM Identity Center-Konsole und API-Autorisierung

Die bestehende IAM Identity Center-Konsole APIs unterstützt die duale Autorisierung, sodass Sie bestehende API-Operationen weiterhin verwenden können, wenn neuere verfügbar APIs 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

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

Name des Konsolenvorgangs, der vor dem 15. November 2023 verwendet wurde	API-Aktion, die nach dem 15. November 2023 verwendet wurde
DeleteSSO	DeleteInstance
DisassociateProfile	DeleteApplicationAssignment
GetApplicationTemplate	DescribeApplicationProvider
GetManagedApplicationInstance	DescribeApplication
GetSharedSsoConfiguration	DescribeInstance
ListApplicationInstances	ListApplications
ListApplicationTemplates	ListApplicationProviders
ListDirectoryAssociations	DescribeInstance
ListProfileAssociations	ListApplicationAssignments
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

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
CreatePermissionSet	CreatePermissionSet	CreatePermissionSet
DeleteApplicationInstanceForAWsAccount	DeleteApplicationInstance | DeleteTrust	DeleteAccountAssignment
DeleteApplicationProfileForAwsAccount	DeleteProfile	DeleteAccountAssignment
DeletePermissionsPolicy	DeletePermissionsPolicy	DeleteInlinePolicyFromPermissionSet
DeletePermissionSet	DeletePermissionSet	DeletePermissionSet
DescribePermissionsPolicies	DescribePermissionsPolicies	ListManagedPoliciesInPermissionSet
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

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
ListPermissionSets	ListPermissionSets	ListPermissionSets
ListProfileAssociations	ListProfileAssociations	ListAccountAssignments
ProvisionApplicationInstanceForAWSAccount	GetApplicationInstance | CreateApplicationInstance	CreateAccountAssignment
ProvisionApplicationProfileForAWSAccountInstance	GetProfile | CreateProfile | UpdateProfile	CreateAccountAssignment
ProvisionSAMLProvider	GetTrust | CreateTrust | UpdateTrust	CreateAccountAssignment
PutPermissionsPolicy	PutPermissionsPolicy	PutInlinePolicyToPermissionSet
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-Emittenten 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

Identitätscenter: 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

Eine bewährte Methode besteht darin, Ihr Unternehmen zu überwachen, um sicherzustellen, dass Änderungen protokolliert werden. Mithilfe der Überwachung können Sie sicherstellen, dass Sie alle unerwarteten Änderungen untersuchen und unerwünschte Änderungen rückgängig machen können. IAM Identity Center unterstützt derzeit zwei AWS Dienste, mit denen Sie Ihr Unternehmen und die darin stattfindenden Aktivitäten überwachen können: AWS CloudTrail und Amazon EventBridge.

Themen

- Protokollieren von IAM Identity Center-API-Aufrufen mit AWS CloudTrail
- Protokollierung von IAM Identity Center-SCIM-API-Aufrufen mit AWS CloudTrail

- Anwendungskomponenten mit Amazon Connect EventBridge
- Protokollierung konfigurierbarer AD-Synchronisierungsfehler

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.

In der folgenden Tabelle sind die CloudTrail Ereignisse von IAM Identity Center, ihre CloudTrail Ereignisquellen und der Abgleich zusammengefasst. APIs Weitere Informationen zu finden Sie in den IAM Identity Center-API-Referenzen. APIs

> **Note**
>
> Es gibt eine weitere Gruppe von CloudTrail Ereignissen, die als Sign-In bezeichnet werden. Diese werden ausgegeben, AWS wenn Sie sich AWS als IAM Identity Center-Benutzer anmelden. Für diese Ereignisse gibt es kein passendes öffentliches APIs Ereignis und sie sind daher nicht in den API-Referenzen aufgeführt.

CloudTrail Ereignisse	Öffentlich APIs	Description	CloudTrail Quellen der Ereignisse
IAM Identity Center	IAM Identity Center	Das IAM Identity Center APIs ermöglicht die	`sso.amazonaws.com`

CloudTrail Ereignisse	Öffentlich APIs	Description	CloudTrail Quellen der Ereignisse
		Verwaltung von Berechtigungssätze n, Anwendung en, vertrauen swürdigen Token-Aus stellern, Konto- und Anwendungszuweisun gen, IAM Identity Center-Instanzen und Tags.	
Identitätsspeicher	Identitätsspeicher	Der Identity Store APIs ermöglich t die Verwaltun g des Lebenszyk lus der Benutzer und Gruppen Ihrer Belegschaft sowie der Gruppenmitgliedsch aften der Benutzer. Außerdem unterstüt zen sie die Verwaltun g der MFA-Geräte der Benutzer.	`sso-direc tory.amaz onaws.com` , `identitys tore.amaz onaws.com`

CloudTrail Ereignisse	Öffentlich APIs	Description	CloudTrail Quellen der Ereignisse
OIDC	OIDC	Das OIDC APIs unterstützt die Weitergabe vertrauen swürdiger Identitäten und die Anmeldung bei IDE-Toolkits als bereits authentif izierter IAM Identity Center-Benutzer. AWS CLI	`sso.amazonaws.com` , `sso-oauth.amazonaws.com`
AWS auf das Portal zugreifen	AWS Zugangsportal	Das AWS Zugriffsportal APIs unterstützt den Betrieb des AWS Zugriffsportals und Benutzer, die Kontoanmeldeinformationen über das abrufen AWS CLI.	`sso.amazonaws.com`
SCIM	ABZOCK	Das SCIM APIs unterstützt die Bereitstellung von Benutzern, Gruppen und Gruppenmitgliedschaften über das SCIM-Protokoll. Weitere Informationen finden Sie unter Protokollierung von IAM Identity Center-SCIM-API-Aufrufen mit AWS CloudTrail.	`identitystore-scim.amazonaws.com`

CloudTrail Ereignisse	Öffentlich APIs	Description	CloudTrail Quellen der Ereignisse
AWS-Anmeldung	Keine öffentliche API	AWS sendet CloudTrail Anmeldeereignisse zur Benutzerauthentifizierung aus und der Verbund fließt in das IAM Identity Center.	`signin.amazon.com`

Themen

- CloudTrail Anwendungsfälle für IAM Identity Center
- IAM Identity Center-Informationen in CloudTrail

CloudTrail Anwendungsfälle für IAM Identity Center

Die CloudTrail Ereignisse, die IAM Identity Center ausgibt, können für eine Vielzahl von Anwendungsfällen nützlich sein. Organizations können diese Ereignisprotokolle verwenden, um den Benutzerzugriff und die Benutzeraktivitäten in ihrer AWS Umgebung zu überwachen und zu prüfen. Dies kann bei Anwendungsfällen zur Einhaltung von Vorschriften hilfreich sein, da in den Protokollen Informationen darüber erfasst werden, wer wann auf welche Ressourcen zugreift. Sie können die CloudTrail Daten auch für die Untersuchung von Vorfällen verwenden, sodass Teams Benutzeraktionen analysieren und verdächtiges Verhalten verfolgen können. Darüber hinaus kann der Ereignisverlauf bei der Problembehebung helfen und bietet Einblick in Änderungen, die im Laufe der Zeit an Benutzerberechtigungen und Konfigurationen vorgenommen wurden.

In den folgenden Abschnitten werden die grundlegenden Anwendungsfälle beschrieben, die Ihre Workflows wie Audits, Untersuchung von Vorfällen und Problembehebung beeinflussen.

Identifizieren des Benutzers in von Benutzern ausgelösten Ereignissen in IAM Identity Center CloudTrail

IAM Identity Center gibt zwei CloudTrail Felder aus, mit denen Sie den IAM Identity Center-Benutzer identifizieren können, der hinter den CloudTrail Ereignissen steht, z. B. der Anmeldung bei IAM Identity Center oder der Nutzung des AWS Zugriffsportals AWS CLI, einschließlich der Verwaltung von MFA-Geräten:

- `userId`— Die eindeutige und unveränderliche Benutzer-ID aus dem Identity Store einer IAM Identity Center-Instanz.
- `identityStoreArn`— Der Amazon-Ressourcenname (ARN) des Identity Store, der den Benutzer enthält.

Die `identityStoreArn` Felder `userID` und werden in dem innerhalb des `onBehalfOf` Elements verschachtelten `userIdentity`Element angezeigt, wie im folgenden CloudTrail Beispiel-Ereignisprotokoll dargestellt. In diesem Ereignisprotokoll werden diese beiden Felder bei einem Ereignis angezeigt, dessen `userIdentity` Typ "`IdentityCenterUser`" ist. Sie finden diese Felder auch bei Ereignissen für authentifizierte IAM Identity Center-Benutzer, bei denen der `userIdentity` Typ "" Unknown ist. Ihre Workflows sollten beide Typwerte akzeptieren.

```
"userIdentity":{
  "type":"IdentityCenterUser",
  "accountId":"111122223333",
  "onBehalfOf": {
    "userId": "544894e8-80c1-707f-60e3-3ba6510dfac1",
    "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
    },
    "credentialId" : "90e292de-5eb8-446e-9602-90f7c45044f7"
  }
```

Tip

Wir empfehlen Ihnen, `userId` und zu verwenden, `identityStoreArn` um den Benutzer zu identifizieren, der hinter IAM Identity CloudTrail Center-Ereignissen steht. Die `principalId` Felder `userName` und unter dem `userIdentity` Element sind nicht mehr verfügbar. Wenn Ihre Workflows, z. B. für Audits oder die Reaktion auf Vorfälle, davon abhängen, dass Sie Zugriff auf das haben`username`, haben Sie zwei Möglichkeiten:

- Rufen Sie den Benutzernamen aus dem IAM Identity Center-Verzeichnis ab, wie unter beschriebenBenutzername bei Anmeldeereignissen CloudTrail.
- Rufen Sie den aus`UserName`, den IAM Identity Center unter dem `additionalEventData` Element Sign-in ausgibt. Für diese Option ist kein Zugriff auf das IAM Identity Center-Verzeichnis erforderlich. Weitere Informationen finden Sie unter Benutzername bei Anmeldeereignissen CloudTrail.

Um die Details eines Benutzers, einschließlich des `username` Felds, abzurufen, fragen Sie den Identity Store mit Benutzer-ID und Identity Store-ID als Parametern ab. Sie können diese Aktion über die `DescribeUser`API-Anfrage oder über die CLI ausführen. Im Folgenden finden Sie ein Beispiel für einen CLI-Befehl. Sie können den `region` Parameter weglassen, wenn sich Ihre IAM Identity Center-Instanz in der CLI-Standardregion befindet.

```
aws identitystore describe-user \
--identity-store-id  d-1234567890 \
--user-id  544894e8-80c1-707f-60e3-3ba6510dfac1 \
--region your-region-id
```

Um den Identity Store ID-Wert für den CLI-Befehl im vorherigen Beispiel zu ermitteln, können Sie die Identity Store ID aus dem `identityStoreArn` Wert extrahieren. Im Beispiel ARN lautet `arn:aws:identitystore::111122223333:identitystore/d-1234567890` die Identity Store-ID`d-1234567890`. Alternativ können Sie die Identity Store-ID finden, indem Sie im Bereich Einstellungen der IAM Identity Center-Konsole zur Registerkarte Identity Store navigieren.

Wenn Sie die Suche nach Benutzern im IAM Identity Center-Verzeichnis automatisieren, empfehlen wir Ihnen, die Häufigkeit der Benutzersuchen abzuschätzen und die IAM Identity Center-Drosselbegrenzung für die Identity Store-API zu berücksichtigen. Das Zwischenspeichern von abgerufenen Benutzerattributen kann Ihnen helfen, die Drosselung einzuhalten.

Korrelieren von Benutzerereignissen innerhalb derselben Benutzersitzung

Das bei Anmeldeereignissen ausgegebene `AuthWorkflowID`Feld ermöglicht die Nachverfolgung aller CloudTrail Ereignisse im Zusammenhang mit einer Anmeldesequenz vor Beginn einer IAM Identity Center-Benutzersitzung.

Für Benutzeraktionen innerhalb des AWS Zugriffsportals wird der `credentialId` Wert auf die ID der Sitzung des IAM Identity Center-Benutzers gesetzt, mit der die Aktion angefordert wurde. Sie können diesen Wert verwenden, um CloudTrail Ereignisse zu identifizieren, die innerhalb derselben authentifizierten IAM Identity Center-Benutzersitzung im Zugriffsportal ausgelöst wurden. AWS

> **Note**
>
> Sie können ihn nicht verwenden`credentialId`, um Anmeldeereignisse mit nachfolgenden Ereignissen, wie z. B. der Nutzung des Zugangsportals, zu korrelieren. AWS Der Wert des `credentialId` Felds, der bei Anmeldeereignissen ausgegeben wird, wird intern verwendet, und wir empfehlen, dass Sie sich nicht darauf verlassen. Der Wert des `credentialId`

Felds, das für mit OIDC aufgerufene AWS Access-Portal-Ereignisse ausgegeben wird, entspricht der ID des Zugriffstokens.

Identifizieren von Sitzungsdetails im Hintergrund von Benutzern in von IAM Identity Center ausgelösten Ereignissen CloudTrail

Das folgende CloudTrail Ereignis erfasst den Prozess des OAuth 2.0-Tokenaustauschs, bei dem ein vorhandenes Zugriffstoken (das`subjectToken`), das die interaktive Sitzung des Benutzers darstellt, gegen ein Aktualisierungstoken (das`requestedTokenType`) ausgetauscht wird. Mit dem Aktualisierungstoken können alle vom Benutzer initiierten Jobs mit langer Laufzeit weiterhin mit den Benutzerberechtigungen ausgeführt werden, auch wenn sich der Benutzer abmeldet.

Bei Hintergrundsitzungen von IAM Identity Center-Benutzern umfasst das CloudTrail Ereignis ein zusätzliches Element, das `resource` `requestParameters` im Element aufgerufen wird. Der `resource` Parameter enthält den Amazon-Ressourcennamen (ARN) des Jobs, der im Hintergrund ausgeführt wird. Dieses Element ist nur in CloudTrail Ereignisdatensätzen vorhanden und nicht in den IAM-API- oder SDK-Antworten von CreateTokenWithIAM Identity Center enthalten.

```
{
  "clientId": "EXAMPLE-CLIENT-ID",
  "grantType": "urn:ietf:params:oauth:grant-type:token-exchange",
  "code": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "redirectUri": "https://example.com/callback",
  "assertion": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "subjectToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "subjectTokenType": "urn:ietf:params:oauth:token-type:access_token",
  "requestedTokenType": "urn:ietf:params:oauth:token-type:refresh_token",
  "resource": "arn:aws:sagemaker:us-west-2:123456789012:training-job/my-job"
}
```

Korrelierung von Benutzern zwischen IAM Identity Center und externen Verzeichnissen

IAM Identity Center bietet zwei Benutzerattribute, mit denen Sie einen Benutzer in seinem Verzeichnis demselben Benutzer in einem externen Verzeichnis zuordnen können (z. B. und). Microsoft Active Directory Okta Universal Directory

- `externalId`— Die externe ID eines IAM Identity Center-Benutzers. Wir empfehlen, diese ID einer unveränderlichen Benutzer-ID im externen Verzeichnis zuzuordnen. Beachten Sie, dass IAM Identity Center diesen Wert nicht in ausgibt. CloudTrail

- `username`— Ein vom Kunden bereitgestellter Wert, mit dem sich Benutzer normalerweise anmelden. Der Wert kann sich ändern (z. B. bei einem SCIM-Update). Beachten Sie, dass, wenn die Identitätsquelle ist Directory Service, der Benutzername, den IAM Identity Center ausgibt, mit dem Benutzernamen CloudTrail übereinstimmt, den Sie zur Authentifizierung eingeben. Der Benutzername muss nicht exakt mit dem Benutzernamen im IAM Identity Center-Verzeichnis übereinstimmen.

  Wenn Sie Zugriff auf die CloudTrail Ereignisse, aber nicht auf das IAM Identity Center-Verzeichnis haben, können Sie den bei der Anmeldung unter dem `additionalEventData` Element angegebenen Benutzernamen verwenden. Weitere Informationen zum Benutzernamen in finden Sie `additionalEventData` unter. Benutzername bei Anmeldeereignissen CloudTrail

Die Zuordnung dieser beiden Benutzerattribute zu den entsprechenden Benutzerattributen in einem externen Verzeichnis ist in IAM Identity Center definiert, wenn die Identitätsquelle der Directory Service ist. Weitere Informationen finden Sie unter. Attributzuordnungen zwischen dem IAM Identity Center und dem Verzeichnis externer Identitätsanbieter Externe Benutzer IdPs , die SCIM bereitstellen, haben ihre eigene Zuordnung. Selbst wenn Sie das IAM Identity Center-Verzeichnis als Identitätsquelle verwenden, können Sie das `externalId` Attribut verwenden, um Sicherheitsprinzipale mit Ihrem externen Verzeichnis zu verknüpfen.

Im folgenden Abschnitt wird erklärt, wie Sie anhand des Benutzernamens und nach einem IAM Identity Center-Benutzer suchen können. `username` `externalId`

Einen IAM Identity Center-Benutzer anhand seines Benutzernamens und seiner externen ID anzeigen

Sie können Benutzerattribute für einen bekannten Benutzernamen aus dem IAM Identity Center-Verzeichnis abrufen, indem Sie zunächst `userId` mithilfe der `GetUserId`API-Anfrage eine entsprechende Anfrage anfordern und dann eine `DescribeUser`API-Anfrage stellen, wie im vorherigen Beispiel gezeigt. Das folgende Beispiel zeigt, wie Sie eine `userId` aus dem Identity Store für einen bestimmten Benutzernamen abrufen können. Sie können den `region` Parameter weglassen, wenn sich Ihre IAM Identity Center-Instanz mit der CLI in der Standardregion befindet.

```
aws identitystore get-user-id \
    --identity-store d-9876543210 \
    --alternate-identifier '{
      "UniqueAttribute": {
      "AttributePath": "username",
      "AttributeValue": "anyuser@example.com"
```

```
        }
          }' \
    --region your-region-id
```

Ebenso können Sie denselben Mechanismus verwenden, wenn Sie den kennen. `externalId` Aktualisieren Sie den Attributpfad im vorherigen Beispiel mit dem `externalId` Wert und den Attributwert mit dem spezifischen `externalId` Wert, nach dem Sie suchen.

Den Secure Identifier (SID) eines Benutzers in Microsoft Active Directory (AD) und ExternalID anzeigen

In bestimmten Fällen gibt IAM Identity Center die SID eines Benutzers im `principalId` Bereich CloudTrail Ereignisse aus, z. B. diejenigen, die das AWS Access Portal und APIs OIDC ausgeben. Diese Fälle werden schrittweise eingestellt. Wir empfehlen, dass Ihre Workflows das AD-Attribut verwendenobjectguid, wenn Sie eine eindeutige Benutzer-ID von AD benötigen. Sie finden diesen Wert im `externalId` Attribut im IAM Identity Center-Verzeichnis. Wenn Ihre Workflows jedoch die Verwendung von SID erfordern, rufen Sie den Wert aus AD ab, da er nicht über IAM Identity Center verfügbar ist. APIs

Korrelieren von Benutzerereignissen innerhalb derselben Benutzersitzungbeschreibt, wie Sie die `username` Felder `externalId` und verwenden können, um einen IAM Identity Center-Benutzer einem passenden Benutzer in einem externen Verzeichnis zuzuordnen. Standardmäßig ist IAM Identity Center dem `objectguid` Attribut in AD `externalId` zugeordnet, und diese Zuordnung ist behoben. IAM Identity Center bietet Administratoren die Flexibilität, eine `username` andere Zuordnung als die Standardzuweisung `userprincipalname` in AD vorzunehmen.

Sie können diese Zuordnungen in der IAM Identity Center-Konsole anzeigen. Navigieren Sie in den Einstellungen zur Registerkarte „Identitätsquelle“ und wählen Sie im Menü „Aktionen“ die Option Synchronisierung verwalten aus. Wählen Sie im Bereich „Synchronisation verwalten“ die Schaltfläche „Attributzuordnungen anzeigen“.

Sie können zwar jede eindeutige AD-Benutzer-ID verwenden, die in IAM Identity Center verfügbar ist, um nach einem Benutzer in AD zu suchen, wir empfehlen jedoch, die `objectguid` in Ihren Abfragen zu verwenden, da es sich um eine unveränderliche Kennung handelt. Das folgende Beispiel zeigt, wie Microsoft AD mit Powershell abgefragt wird, um einen Benutzer mit dem `objectguid` Benutzerwert von `16809ecc-7225-4c20-ad98-30094aefdbca` abzurufen. Eine erfolgreiche Antwort auf diese Abfrage beinhaltet die SID des Benutzers.

```
Install-WindowsFeature -Name  RSAT-AD-PowerShell
```

```
Get-ADUser `
-Filter {objectGUID -eq  [GUID]::Parse("16809ecc-7225-4c20-ad98-30094aefdbca")} `
-Properties *
```

IAM Identity Center-Informationen in 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.

> **Note**
>
> Weitere Informationen zur Entwicklung der Benutzeridentifikation und Nachverfolgung von Benutzeraktionen bei CloudTrail Ereignissen finden Sie im AWS Sicherheitsblog unter Wichtige Änderungen an CloudTrail Ereignissen für IAM Identity Center.

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 in folgenden Themen im AWS CloudTrail -Benutzerhandbuch:

- 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.

CloudTrail Ereignisse für das unterstützte IAM Identity Center APIs

Die folgenden Abschnitte enthalten Informationen zu den CloudTrail Ereignissen im Zusammenhang mit den folgenden Ereignissen APIs , die IAM Identity Center unterstützt:

- IAM Identity Center-API
- Identitätsspeicher-API
- OIDC-API
- AWS auf die Portal-API zugreifen
- SCIM-API

CloudTrail Ereignisse im Zusammenhang mit IAM Identity Center API-Vorgängen

Die folgende Liste enthält die CloudTrail Ereignisse, die die öffentlichen IAM Identity Center-Operationen zusammen mit der `sso.amazonaws.com` Ereignisquelle auslösen. Weitere Informationen zu den öffentlichen IAM Identity Center-API-Vorgängen finden Sie in der IAM Identity Center API-Referenz.

Möglicherweise finden Sie weitere Ereignisse CloudTrail für API-Operationen der IAM Identity Center-Konsole, auf die sich die Konsole stützt. Weitere Informationen zu diesen Konsolen APIs finden Sie in der Service Authorization Reference.

- AttachCustomerManagedPolicyReferenceToPermissionSet
- AttachManagedPolicyToPermissionSet
- CreateAccountAssignment
- CreateApplication
- CreateApplicationAssignment

- CreateInstance
- CreateInstanceAccessControlAttributeConfiguration
- CreatePermissionSet
- CreateTrustedTokenIssuer
- DeleteAccountAssignment
- DeleteApplication
- DeleteApplicationAccessScope
- DeleteApplicationAssignment
- DeleteApplicationAuthenticationMethod
- DeleteApplicationGrant
- DeleteInlinePolicyFromPermissionSet
- DeleteInstance
- DeleteInstanceAccessControlAttributeConfiguration
- DeletePermissionsBoundaryFromPermissionSet
- DeletePermissionSet
- DeleteTrustedTokenIssuer
- DescribeAccountAssignmentCreationStatuss
- DescribeAccountAssignmentDeletionStatus

- DescribeApplication
- DescribeApplicationAssignment
- DescribeApplicationProvider
- DescribeInstance
- DescribeInstanceAccessControlAttributeConfiguration
- DescribePermissionSet
- DescribePermissionSetProvisioningStatus
- DescribeTrustedTokenIssuer
- DetachCustomerManagedPolicyReferenceFromPermissionSet
- DetachManagedPolicyFromPermissionSet
- GetApplicationAccessScope
- GetApplicationAssignmentConfiguration
- GetApplicationAuthenticationMethod
- GetApplicationGrant
- GetInlinePolicyForPermissionSet
-

GetPermissionsBoundaryForPermissionSet

- ListAccountAssignmentCreationStatus
- ListAccountAssignmentDeletionStatus
- ListAccountAssignments
- ListAccountAssignmentsForPrincipal
- ListAccountsForProvisionedPermissionSet
- ListApplicationAccessScopes
- ListApplicationAssignments
- ListApplicationAssignmentsForPrincipal
- ListApplicationAuthenticationMethods
- ListApplicationGrants
- ListApplicationProviders
- ListApplications
- ListCustomerManagedPolicyReferencesInPermissionSet
- ListInstances
-

ListManagedPoliciesInPermissionSet

- ListPermissionSetProvisioningStatus
- ListPermissionSets
- ListPermissionSetsProvisionedToAccount
- ListTagsForResource
- ListTrustedTokenIssuers
- ProvisionPermissionSet
- PutApplicationAccessScope
- PutApplicationAssignmentConfiguration
- PutApplicationAuthenticationMethod
- PutApplicationGrant
- PutInlinePolicyToPermissionSet
- PutPermissionsBoundaryToPermissionSet
- TagResource
- UntagResource
-

- UpdateApplication
- UpdateInstance
- UpdateInstanceAccessControlAttributeConfiguration
- UpdatePermissionSet
- UpdateTrustedTokenIssuer

CloudTrail Ereignisse von Identity Store API-Vorgängen

Die folgende Liste enthält die CloudTrail Ereignisse, die die öffentlichen Identity Store-Operationen zusammen mit der `identitystore.amazonaws.com` Ereignisquelle auslösen. Weitere Informationen zu den öffentlichen Identity Store-API-Vorgängen finden Sie in der Identity Store-API-Referenz.

Möglicherweise finden Sie weitere Ereignisse CloudTrail für die API-Operationen der Identity Store-Konsole mit der `sso-directory.amazonaws.com` Ereignisquelle. Diese APIs unterstützen die Konsole und das AWS Zugriffsportal. Wenn Sie das Auftreten eines bestimmten Vorgangs erkennen müssen, z. B. das Hinzufügen eines Mitglieds zu einer Gruppe, empfehlen wir Ihnen, sowohl öffentliche als auch Konsolen-API-Operationen in Betracht zu ziehen. Weitere Informationen zu diesen Konsolen APIs finden Sie in der Service Authorization Reference.

- CreateGroup
- CreateGroupMembership
- CreateUser
- DeleteGroup
- DeleteGroupMembership
- DeleteUser
- DescribeGroup
- DescribeGroupMembership
- DescribeUser
- GetGroupId

- GetGroupMembershipId
- GetUserId
- IsMemberInGroups
- ListGroupMemberships
- ListGroupMembershipsForMember
- ListGroups
- ListUsers
- UpdateGroup
- UpdateUser

CloudTrail Ereignisse von OIDC-API-Vorgängen

Die folgende Liste enthält die CloudTrail Ereignisse, die die öffentlichen OIDC-Operationen auslösen. Weitere Informationen zu den öffentlichen OIDC-API-Vorgängen finden Sie in der OIDC-API-Referenz.

- CreateToken(Quelle des Ereignisses) `sso.amazonaws.com`
- CreateTokenWithIAM(Ereignisquelle`sso-oauth.amazonaws.com`)

CloudTrail Ereignisse im Zusammenhang mit API-Vorgängen des AWS Zugriffsportals

Die folgende Liste enthält die CloudTrail Ereignisse, die von den API-Vorgängen des AWS Zugriffsportals mit der `sso.amazonaws.com` Ereignisquelle ausgelöst werden. Die API-Operationen, die in der öffentlichen API als nicht verfügbar eingestuft wurden, unterstützen den Betrieb des AWS Zugriffsportals. Die Verwendung von AWS CLI kann dazu führen, dass CloudTrail Ereignisse sowohl bei den API-Vorgängen des öffentlichen AWS Zugriffsportals als auch bei Vorgängen, die in der öffentlichen API nicht verfügbar sind, ausgelöst werden. Weitere Informationen zu API-Vorgängen im Portal für AWS den öffentlichen Zugriff finden Sie in der API-Referenz für das AWS Zugangsportal.

- Authenticate(In der öffentlichen API nicht verfügbar. Ermöglicht die Anmeldung zum AWS Zugriffsportal.)
- Federate(In der öffentlichen API nicht verfügbar. Ermöglicht den Zusammenschluss von Anwendungen.)
- ListAccountRoles

- ListAccounts
- ListApplications(In der öffentlichen API nicht verfügbar. Stellt Benutzern zugewiesene Ressourcen zur Anzeige im AWS Access-Portal bereit.)
- ListProfilesForApplication(In der öffentlichen API nicht verfügbar. Stellt Anwendungsmetadaten zur Anzeige im AWS Access-Portal bereit.)
- GetRoleCredentials
- Logout

CloudTrail Ereignisse von SCIM-API-Vorgängen

Informationen zu öffentlichen SCIM-API-Vorgängen finden Sie unter API-Referenz für das AWS Access Portal.

Identitätsinformationen bei IAM Identity Center-Ereignissen CloudTrail

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.
- Ob die Anfrage von einem IAM Identity Center-Benutzer gestellt wurde. Falls ja, sind die `identityStoreArn` Felder `userId` und in den CloudTrail Ereignissen verfügbar, um den IAM Identity Center-Benutzer zu identifizieren, der die Anfrage initiiert hat. Weitere Informationen finden Sie unter Identifizieren des Benutzers in von Benutzern ausgelösten Ereignissen in IAM Identity Center CloudTrail .

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

> **Note**
>
> Derzeit sendet IAM Identity Center keine CloudTrail Ereignisse für die Benutzeranmeldung bei AWS verwalteten Webanwendungen (z. B. Amazon SageMaker AI Studio) mit der OIDC-API aus. Diese Webanwendungen sind Teil der breiteren Palette vonthe section called “AWS

verwaltete Anwendungen”, zu denen auch Nicht-Webanwendungen wie Amazon Athena SQL und Amazon S3 Access Grants gehören.

CloudTrail Ereignisse für IAM Identity Center verstehen

Ein Trail ist eine Konfiguration, durch die Ereignisse an den von Ihnen angegebenen Amazon-S3-Bucket übermittelt werden. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Ereignisse sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden. Weitere Informationen zum Inhalt eines CloudTrail Datensatzes finden Sie im CloudTrail Benutzerhandbuch.

Dieses Beispiel zeigt einen CloudTrail Protokolleintrag, der eine `DescribePermissionsPolicies` Aktion aufzeichnet, die von einem IAM-Benutzer (samadams) ausgeführt wurde, der mit IAM Identity Center interagiert:


```
{
   "Records":[
      {
         "eventVersion":"1.05",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDAJAIENLMexample",
            "arn":"arn:aws:iam::08966example:user/samadams",
            "accountId":"111122223333",
            "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":"111122223333"
      }
   ]
}
```

Dieses Beispiel zeigt einen CloudTrail Protokolleintrag, der eine `ListApplications` Aktion aufzeichnet, die von einem IAM Identity Center-Benutzer im Zugriffsportal ausgeführt wurde: AWS

```
{
   "Records":[
      {
         "eventVersion":"1.05",
         "userIdentity":{
            "type":"IdentityCenterUser",
            "accountId":"111122223333",
            "onBehalfOf": {
              "userId": "94d00cd8-e9e6-4810-b177-b08e84775435",
              "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
            },
            "credentialId" : "cdee2490-82ed-43b3-96ee-b75fbf0b97a5"
         },
         "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":"111122223333"
      }
   ]
}
```

Dieses Beispiel zeigt einen CloudTrail Protokolleintrag, der eine `CreateToken` Aktion aufzeichnet, die von einem IAM Identity Center-Benutzer ausgeführt wurde, der sich beim IAM Identity Center OIDC-Dienst authentifiziert:


```
{
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IdentityCenterUser",
        "accountId": "111122223333",
        "onBehalfOf": {
          "userId": "94d00cd8-e9e6-4810-b177-b08e84775435",
          "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
        },
        "credentialId" : "cdee2490-82ed-43b3-96ee-b75fbf0b97a5"
      },
      "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": "111122223333",
          "type": "IdentityStoreId",
          "ARN": "d-1234567890"
```

```
        }
      ],
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
}
```

Grundlegendes zu den Anmeldeereignissen bei IAM Identity Center

AWS CloudTrail zeichnet erfolgreiche und erfolglose Anmeldeereignisse für alle IAM Identity Center-Identitätsquellen auf. Identitäten aus IAM Identity Center und Active Directory (AD Connector und AWS Managed Microsoft AD) enthalten zusätzliche Anmeldeereignisse, die jedes Mal erfasst werden, wenn ein Benutzer aufgefordert wird, eine bestimmte Anmeldeanfrage oder einen bestimmten Faktor zu lösen, zusätzlich zum Status dieser speziellen Anforderung 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	Systemeigene IAM Identity Center-Benutzer, AD Connector und AWS Managed Microsoft AD

Ereignisname	Zweck des Ereignisses	Anwendbarkeit der Identitätsquelle
	zu lösen, und gibt an, ob diese Anmeldeinformationen erfolgreich waren oder nicht.	
`UserAuthentication`	Wird verwendet, um zu benachrichtigen, dass alle Authentifizierungsanforderungen, mit denen der Benutzer konfrontiert wurde, erfolgreich erfüllt wurden und dass der Benutzer erfolgreich angemeldet wurde. Wenn Benutzer die erforderlichen Anmeldedaten nicht erfolgreich abschließen, wird kein *`UserAuthentication`* Ereignis protokolliert.	Alle Identitätsquellen

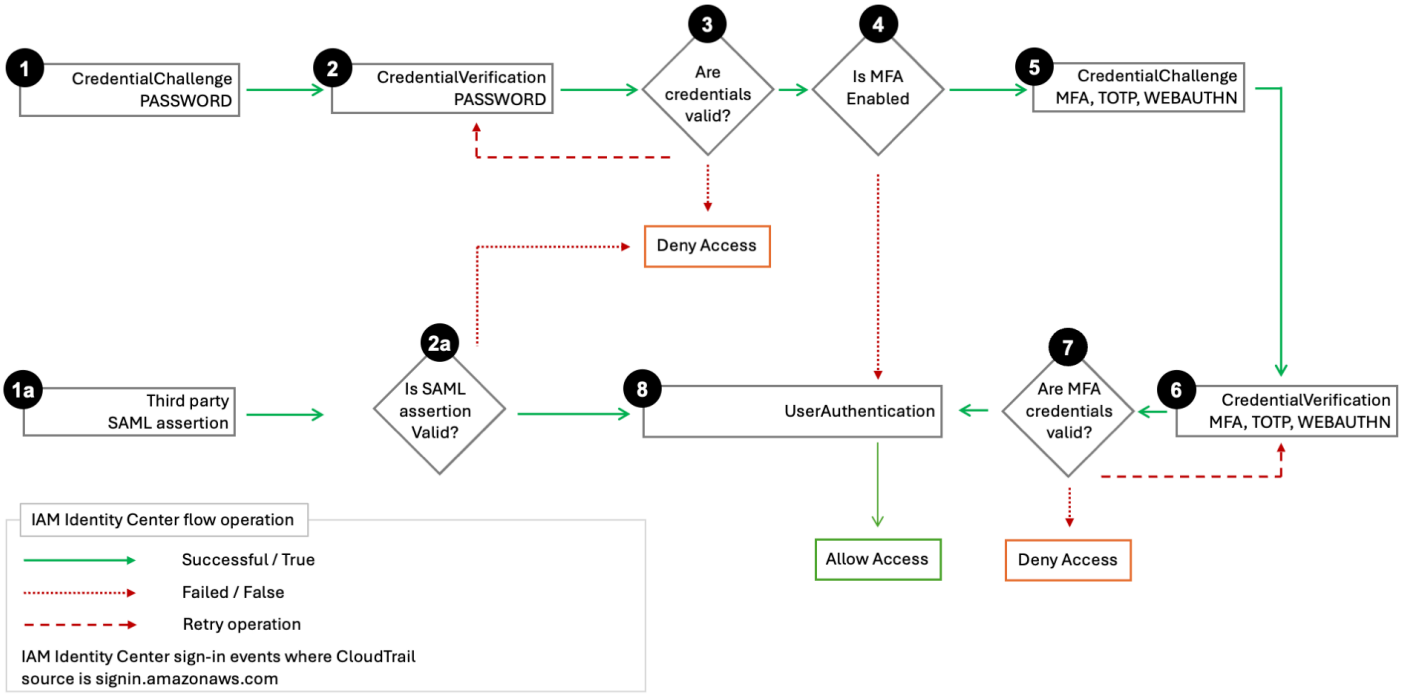
In der folgenden Tabelle werden zusätzliche nützliche Ereignisdatenfelder erfasst, die in bestimmten CloudTrail Anmeldeereignissen enthalten sind.

Feld	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	`CredentialChallenge` , `CredentialVerification` , `UserAuthentication`	„AuthWorkflowID“: „9de74b32-8362-4a01-a524-de21df59fd83"

Feld	Zweck des Ereignisses	Anwendbarkeit des Anmeldeereignisses	Beispielwerte
	IAM Identity Center ausgelöst werden.		
`CredentialType`	Wird verwendet, um den Berechtigungsnachweis oder den Faktor anzugeben, der angefochten wurde. `UserAuthentication` Ereignisse umfassen alle `CredentialType` Werte, die in der Anmeldesequenz des Benutzers erfolgreich verifiziert wurden.	`CredentialChallenge` , `CredentialVerification` , `UserAuthentication`	CredentialType„: „PASSWORD“ oder "„: CredentialType „PASSWORD, TOTP“ (mögliche Werte sind: PASSWORD, TOTP, WEBAUTHN, EXTERNAL_IDP, RESYNC_TOTP, EMAIL_OTP)
`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/....."

CloudTrail Ereignisse in den Anmeldeabläufen von IAM Identity Center

Das folgende Diagramm beschreibt den Anmeldeablauf und die CloudTrail Ereignisse, die bei der Anmeldung ausgelöst werden.



Das Diagramm zeigt einen Ablauf für die Kennwortanmeldung und einen Verbundanmeldeablauf.

Der Ablauf der Kennwortanmeldung, der aus den Schritten 1—8 besteht, veranschaulicht die Schritte während des Anmeldevorgangs mit Benutzername und Passwort. IAM Identity Center wird `userIdentity.additionalEventData.CredentialType` auf "`PASSWORD`" gesetzt, und IAM Identity Center durchläuft den Challenge-Response-Zyklus für die Anmeldeinformationen und versucht es bei Bedarf erneut.

Die Anzahl der Schritte hängt von der Art der Anmeldung und dem Vorhandensein der Multi-Faktor-Authentifizierung (MFA) ab. Der anfängliche Vorgang führt zu drei oder fünf CloudTrail Ereignissen, wobei die Sequenz für eine erfolgreiche Authentifizierung `UserAuthentication` beendet wird. Erfolglose Versuche zur Passwortauthentifizierung führen zu zusätzlichen CloudTrail Ereignissen, da das IAM Identity Center die reguläre Authentifizierung oder, falls aktiviert, die MFA-Authentifizierung erneut ausgibt`CredentialChallenge`.

Der Ablauf der Passwort-Anmeldung deckt auch das Szenario ab, in dem sich ein IAM Identity Center-Benutzer, der mit einem `CreateUser` API-Aufruf neu erstellt wurde, mit einem Einmalpasswort (OTP) anmeldet. Der Anmeldeinformationstyp in diesem Szenario ist „“. `EMAIL_OTP`

Der föderierte Anmeldeablauf, der aus den Schritten 1a, 2a und 8 besteht, veranschaulicht die wichtigsten Schritte während des Verbundauthentifizierungsprozesses, bei dem eine SAML-Assertion von einem Identitätsanbieter bereitgestellt und vom IAM Identity Center validiert wird. Falls erfolgreich, führt dies zu. `UserAuthentication` IAM Identity Center ruft die interne MFA-Authentifizierungssequenz in den Schritten 3 bis 7 nicht auf, da ein externer, föderierter Identitätsanbieter für die gesamte Authentifizierung von Benutzeranmeldeinformationen verantwortlich ist.

Benutzername bei Anmeldeereignissen CloudTrail

IAM Identity Center gibt das `UserName` Feld unter dem `additionalEventData` Element einmal pro erfolgreicher Anmeldung eines IAM Identity Center-Benutzers aus. In der folgenden Liste werden der Umfang der beiden Anmeldeereignisse und die Bedingungen, unter denen diese Ereignisse auftreten, beschrieben. Nur eine der Bedingungen kann erfüllt sein, wenn sich ein Benutzer anmeldet.

- `CredentialChallenge`
  - Wann `CredentialType` ist "`PASSWORD`" — gilt für die Passwortauthentifizierung mit Directory Service oder IAM-Identity-Center-Verzeichnis.
  - Wann `CredentialType` ist "`EMAIL_OTP`" — gilt nur für den IAM-Identity-Center-Verzeichnis Fall, dass ein mit einem `CreateUser` API-Aufruf erstellter Benutzer versucht, sich zum ersten Mal anzumelden, und der Benutzer ein Einmalkennwort erhält, mit dem er sich einmal mit diesem Passwort anmelden kann.
- `UserAuthentication`
  - Wann `CredentialType` ist "`EXTERNAL_IDP`" — gilt für die Authentifizierung mit einem externen IdP.

Der Wert von `UserName` für erfolgreiche Authentifizierungen lautet wie folgt:

- Wenn die Identitätsquelle ein externer IdP ist, entspricht der Wert dem `nameID` Wert in der eingehenden SAML-Assertion. Dieser Wert entspricht dem `UserName` Feld in der. IAM-Identity-Center-Verzeichnis
- Wenn die Identitätsquelle ein ist IAM-Identity-Center-Verzeichnis, entspricht der ausgegebene Wert dem `UserName` Feld in diesem Verzeichnis.

- Wenn die Identitätsquelle der ist Directory Service, entspricht der ausgegebene Wert dem Benutzernamen, den der Benutzer bei der Authentifizierung eingibt. Beispielsweise kann sich ein Benutzer, der den Benutzernamen hat`anyuser@company.com`, mit`anyuser`, oder authentifizieren `anyuser@company.comcompany.com/anyuser`, und in jedem Fall wird der eingegebene Wert CloudTrail jeweils ausgegeben.

Sicherheitsmaskierung falscher Versuche mit dem Benutzernamen

Das `UserName` Feld enthält die Zeichenfolge, `HIDDEN_DUE_TO_SECURITY_REASONS` wenn es sich bei dem aufgezeichneten Ereignis um einen Anmeldefehler auf der Konsole handelt, der durch eine falsche Eingabe des Benutzernamens verursacht wurde. CloudTrail zeichnet den Inhalt in diesem Fall nicht auf, da der Text vertrauliche Informationen enthalten könnte, wie in den folgenden Beispielen beschrieben:

- Ein Benutzer gibt versehentlich ein Passwort im Feld für den Benutzernamen ein.
- Ein Benutzer gibt versehentlich den Kontonamen eines persönlichen E-Mail-Kontos, eine Bank-Anmelde-ID oder eine andere private ID ein.

> **Tip**
>
> Wir empfehlen Ihnen, `userId` und zu verwenden, `identityStoreArn` um den Benutzer zu identifizieren, der hinter den IAM Identity CloudTrail Center-Ereignissen steht. Wenn Sie das `userName` Feld verwenden müssen, können Sie das Element `userName` unter dem `additionalEventData` Element verwenden, das bei jeder erfolgreichen Anmeldung einmal ausgegeben wird.

Weitere Informationen darüber, wie Sie das `UserName` Feld verwenden können, finden Sie Korrelieren von Benutzerereignissen innerhalb derselben Benutzersitzung unter.

Beispielereignisse für IAM Identity Center-Anmeldeszenarien

Die folgenden Beispiele veranschaulichen die typischen CloudTrail Ereignissequenzen, die während verschiedener AWS Anmeldeszenarien generiert werden. Diese Beispiele dienen als Referenzmuster, anhand derer Sie Authentifizierungsprotokolle interpretieren, Sicherheitsprobleme identifizieren und überprüfen können, ob Ihre Authentifizierungsrichtlinien ordnungsgemäß funktionieren.

Themen

Erfolgreiche Anmeldung, wenn Sie sich nur mit einem Passwort authentifizieren

Die folgende Abfolge von Ereignissen zeigt ein Beispiel für eine erfolgreiche Anmeldung nur mit Passwort.

CredentialChallenge (Passwort)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "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",
      "UserName":"bobsmith@example.com",
      "CredentialType":"PASSWORD"
   },
   "requestID":"5be44ffb-6946-4f47-acaf-1adebd4afead",
   "eventID":"27ea7725-c1fd-4355-bdba-d0e628e0e604",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```

Erfolgreich CredentialVerification (Passwort)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "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":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "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":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "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",
      "UserName":"bobsmith@example.com"
   },
   "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 Authentifizierungs-App mit zeitbasiertem Einmalpasswort (TOTP)

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":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
```

```
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "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",
      "UserName":"bobsmith@example.com"
   },
   "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":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
```

```
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "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":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
```

```
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "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":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
```

```
   },
   "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":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "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 eine erfolgreiche Kennwortauthentifizierung, bei der sich der Benutzer registrieren und die Multi-Faktor-Authentifizierung (MFA) erfolgreich abschließen musste, bevor der Anmeldevorgang abgeschlossen werden konnte.

CredentialChallenge (Passwort)


```
{
   "eventVersion":"1.08",
```

```
   "userIdentity":{
      "type":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "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",
      "UserName":"bobsmith@example.com"
   },
   "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":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "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":"IdentityCenterUser",
      "arn":"",
```

```
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "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 aufgrund einer falschen Passwortauthentifizierung

Die folgende Abfolge von Ereignissen zeigt einen Authentifizierungsversuch, bei dem der Benutzer seinen Benutzernamen erfolgreich eingegeben hat, aber die Passwortverifizierung nicht bestanden hat, was zu einer erfolglosen Anmeldung führte.

CredentialChallenge (Passwort)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
   },
   "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",
      "UserName":"bobsmith@example.com"
   },
   "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",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
   },
   "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"
   }
}
```


Protokollierung von IAM Identity Center-SCIM-API-Aufrufen mit AWS CloudTrail

IAM Identity Center SCIM ist integriert AWS CloudTrail, ein Dienst, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS-Service CloudTrail erfasst API-Aufrufe für SCIM als Ereignisse. Anhand der von CloudTrail gesammelten Informationen können Sie die Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion, die Anforderungsparameter usw. ermitteln. Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

> **Note**
>
> CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Möglicherweise müssen Sie Ihr Zugriffstoken jedoch rotieren, um Ereignisse aus SCIM sehen zu können, wenn Ihr Token vor September 2024 erstellt wurde.
> Weitere Informationen finden Sie unter Ein Zugriffstoken rotieren.

SCIM unterstützt die Protokollierung der folgenden Vorgänge als Ereignisse in: CloudTrail

- CreateGroup
- CreateUser
- DeleteGroup
- DeleteUser
- GetGroup
- GetSchema
- GetUser
- ListGroups
- ListResourceTypes
- ListSchemas
- ListUsers
- PatchGroup
- PatchUser
- PutUser
- ServiceProviderConfig

Beispiele für Ereignisse CloudTrail

Die folgenden Beispiele zeigen typische CloudTrail Ereignisprotokolle, die bei SCIM-Vorgängen mit IAM Identity Center generiert werden. Diese Beispiele zeigen die Struktur und den Inhalt von Ereignissen für erfolgreiche Operationen und häufige Fehlerszenarien und helfen Ihnen zu verstehen, wie CloudTrail Protokolle bei der Behebung von SCIM-Bereitstellungsproblemen zu interpretieren sind.

Erfolgreicher Betrieb **`CreateUser`**

Dieses CloudTrail Ereignis zeigt einen erfolgreichen `CreateUser` Vorgang, der über die SCIM-API ausgeführt wurde. Das Ereignis erfasst sowohl die Anforderungsparameter (wobei vertrauliche Informationen maskiert sind) als auch die Antwortelemente, einschließlich der ID des neu erstellten Benutzers. Dieser Ereignistyp wird generiert, wenn ein Identitätsanbieter erfolgreich einen neuen Benutzer mithilfe des SCIM-Protokolls für IAM Identity Center bereitstellt.


```
{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "WebIdentityUser",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "CreateUser",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "requestParameters": {
    "httpBody": {
      "displayName": "HIDDEN_DUE_TO_SECURITY_REASONS",
      "schemas" : [
        "urn:ietf:params:scim:schemas:core:2.0:User"
      ],
      "name": {
        "familyName": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "givenName": "HIDDEN_DUE_TO_SECURITY_REASONS"
      },
      "active": true,
      "userName": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "tenantId": "xxxx"
  },
  "responseElements": {
    "meta" : {
      "created" : "Oct 10, 2024, 1:23:45 PM",
      "lastModified" : "Oct 10, 2024, 1:23:45 PM",
      "resourceType" : "User"
    },
    "displayName" : "HIDDEN_DUE_TO_SECURITY_REASONS",
```

```
    "schemas" : [
      "urn:ietf:params:scim:schemas:core:2.0:User"
    ],
    "name": {
      "familyName": "HIDDEN_DUE_TO_SECURITY_REASONS",
      "givenName": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "active": true,
    "id" : "c4488478-a0e1-700e-3d75-96c6bb641596",
    "userName": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "requestID": "xxxx",
  "eventID": "xxxx",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
  }
}
```


Fehlgeschlagener **`PatchGroup`** Vorgang: Erforderliches Pfadattribut fehlt

Dieses CloudTrail Ereignis zeigt einen fehlgeschlagenen `PatchGroup` Vorgang, der zu `ValidationException` einer Fehlermeldung geführt hat`"Missing path in PATCH request"`. Der Fehler ist aufgetreten, weil für den `PATCH` Vorgang ein Pfadattribut erforderlich ist, um anzugeben, welches Gruppenattribut geändert werden soll, dieses Attribut jedoch in der Anforderung fehlte.


```
{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "PatchGroup",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xxx.xxx.xxx.xxx",
```

```
  "userAgent": "Go-http-client/2.0",
  "errorCode": "ValidationException",
  "errorMessage": "Missing path in PATCH request",
  "requestParameters": {
    "httpBody": {
      "operations": [
        {
          "op": "REMOVE",
          "value": "HIDDEN_DUE_TO_SECURITY_REASONS"
        }
      ],
      "schemas": [
        "HIDDEN_DUE_TO_SECURITY_REASONS"
      ]
    },
    "tenantId": "xxxx",
    "id": "xxxx"
  },
  "responseElements": null,
  "requestID": "xxxx",
  "eventID": "xxxx",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
  }
}
```


Fehlgeschlagener **`CreateGroup`** Vorgang: Der Gruppenname ist bereits vorhanden

Dieses CloudTrail Ereignis zeigt einen fehlgeschlagenen `CreateGroup` Vorgang, der zu einer `ConflictException` mit der Fehlermeldung geführt hat`"Duplicate GroupDisplayName"`. Dieser Fehler tritt auf, wenn versucht wird, eine Gruppe mit einem Anzeigenamen zu erstellen, der bereits in IAM Identity Center vorhanden ist. Der Identitätsanbieter muss einen eindeutigen Gruppennamen verwenden oder die bestehende Gruppe aktualisieren, anstatt eine neue zu erstellen.


```
{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
```

```
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "CreateGroup",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xxx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "errorCode": "ConflictException",
  "errorMessage": "Duplicate GroupDisplayName",
  "requestParameters": {
    "httpBody": {
      "displayName": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "tenantId": "xxxx"
  },
  "responseElements": null,
  "requestID": "xxxx",
  "eventID": "xxxx",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
  }
}
```


Fehlgeschlagener **`PatchUser`** Vorgang: Mehrere E-Mail-Adressen werden nicht unterstützt

Dieses CloudTrail Ereignis zeigt einen fehlgeschlagenen `PatchUser` Vorgang, der zu einer `ValidationException` mit der Fehlermeldung geführt hat"`List attribute emails exceeds allowed limit of 1`". Dieser Fehler tritt auf, wenn versucht wird, einem Benutzer mehrere E-Mail-Adressen zuzuweisen, da IAM Identity Center nur eine E-Mail-Adresse pro Benutzer unterstützt. Der Identitätsanbieter muss die SCIM-Zuordnung so konfigurieren, dass für jeden Benutzer nur eine einzige E-Mail-Adresse gesendet wird.


```
{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
```

```
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "PatchUser",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xxx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "errorCode": "ValidationException",
  "errorMessage": "List attribute emails exceeds allowed limit of 1",
  "requestParameters": {
    "httpBody": {
      "operations": [
        {
          "op": "REPLACE",
          "path": "emails",
          "value": "HIDDEN_DUE_TO_SECURITY_REASONS"
        }
      ],
      "schemas": [
        "HIDDEN_DUE_TO_SECURITY_REASONS"
      ]
    },
    "tenantId": "xxxx",
    "id": "xxxx"
  },
  "responseElements": null,
  "requestID": "xxxx",
  "eventID": "xxxx",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
  }
}
```

Häufige SCIM-API-Validierungsfehler im IAM Identity Center

Die folgenden Validierungsfehlermeldungen treten häufig in CloudTrail Ereignissen auf, wenn die SCIM-API mit IAM Identity Center verwendet wird. Diese Validierungsfehler treten in der Regel bei der Benutzer- und Gruppenbereitstellung auf.

Ausführliche Anleitungen zur Behebung dieser Fehler und zur ordnungsgemäßen Konfiguration der SCIM-Bereitstellung finden Sie in diesem Artikel.AWS re:Post

- E-Mail mit Listenattribut überschreitet den zulässigen Grenzwert von 1
- Zulässiges Limit für Listenattributadressen von 1
- Es wurden 1 Validierungsfehler festgestellt: Der Wert bei '*name.familyName*' konnte die Einschränkung nicht erfüllen: Das Mitglied muss das Muster eines regulären Ausdrucks erfüllen: [\\ p {L}\\ p {M}\\ p {S}\\ p {N}\\ p {P}\\ t\\n\\ r] +
- Es wurden 2 Validierungsfehler festgestellt: Der Wert in 'Name.FamilyName' konnte die Einschränkung nicht erfüllen: Das Mitglied muss eine Länge größer oder gleich 1 haben; der Wert in 'Name.familyName' konnte die Einschränkung nicht erfüllen: Das Mitglied muss das reguläre Ausdrucksmuster erfüllen: [\\ p {L}\\ p {M}\\ p {S}\\ p {N}\\ p {N}\\ p {P}\\ t\\n\\ r] +
- Es wurden 2 Validierungsfehler festgestellt: Der Wert bei 'urn:IETF:params:scim:schemas:Extension:Enterprise:2.0:user.manager.value' konnte die Einschränkung nicht erfüllen: Der Wert bei 'urn:ietf:params:scim:schemas:Extension:enterprise:2.0:user.manager.value' konnte die Einschränkung nicht erfüllen: Mitglied muss das reguläre Ausdrucksmuster erfüllen: [\\ p {L}\\ p {M}\\ \ p {S}\\ p {N}\\ p {P}\\ t\\n\\ r] +“,
- Ungültiges JSON von RequestBody
- Ungültiges Filterformat

Anwendungskomponenten mit Amazon Connect EventBridge

Sie können IAM Identity Center mit Amazon integrieren, EventBridge um Ereignisse auszulösen, die administrative Benachrichtigungen auslösen oder automatisierte Workflows als Reaktion auf bestimmte IAM Identity Center-Aktionen aufrufen, die in Ereignissen aufgezeichnet wurden. CloudTrail

Sie können beispielsweise EventBridge Regeln konfigurieren, um zu erkennen, wann ein Benutzer eine Anwendung löscht oder wann IAM Identity Center eine neue Gruppe erstellt. Abhängig von Ihrem Anwendungsfall können Sie diese Ereignisse an ein Amazon SNS SNS-Thema weiterleiten,

um Administratoren zu benachrichtigen oder zusätzliche Automatisierungen mithilfe von AWS LambdaStep Functions oder anderen EventBridgeunterstützten Diensten aufzurufen.

Protokollierung konfigurierbarer AD-Synchronisierungsfehler

Sie können die Protokollierung für Ihre konfigurierbaren Active Directory-Synchronisierungskonfigurationen (AD) aktivieren, um Protokolle mit Informationen über Fehler zu erhalten, die während des Synchronisierungsvorgangs auftreten können. Mit diesen Protokollen können Sie überwachen, ob ein Problem mit Ihrer 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 bereitgestellten 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 konfigurierbare AD-Synchronisierungsfehlerprotokolle zu aktivieren

1. Melden Sie sich bei der IAM Identity Center-Konsole an.
2. Wählen Sie 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 konfigurierbare AD-Synchronisierungsfehlerprotokolle zu deaktivieren

1. Melden Sie sich bei der IAM Identity Center-Konsole an.
2. Wählen Sie 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.

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. 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 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. Weitere Informationen zu Ihrer Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services finden Sie in der AWS Sicherheitsdokumentation.

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-Kontrol len vorhanden sind, und das geeignete Verantwor tungsmodell für die Erfüllung der Anforderungen des vom Australian Cyber Security Centre (ACSC) herausgeg ebenen Informationssicherheitshandbuch (ISM) der australischen Regierung festzulegen. Weitere Informati onen finden Sie unter IRAP Resources.
	Das IAM Identity Center verfügt über eine Konformit ätsbescheinigung 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-K onformitätszertifizierung 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.

Datenschutz im IAM Identity Center

Das Modell der AWS gemeinsamen Verantwortung gilt für den Datenschutz in AWS IAM Identity Center. AWS Ist, wie in diesem Modell beschrieben, für den Schutz der globalen Infrastruktur verantwortlich, auf der die gesamte AWS Cloud läuft. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben der von Ihnen verwendeten AWS Dienste verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS-Modell der geteilten Verantwortung und die GDPRAWS im Blog zur -Sicherheit.

Wir empfehlen Ihnen, Ihre Daten auf folgende Weise zu sichern:

- Verwenden Sie die Multi-Faktor-Authentifizierung (MFA) mit IAM Identity Center.
- Verwenden Sie TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen innerhalb der AWS Dienste.

Wir empfehlen dringend, niemals vertrauliche oder sensible Informationen, wie z. B. die E-Mail-Adressen Ihrer Kunden, in Tags oder frei formatierte Textfelder wie ein Namensfeld zu speichern. Dies gilt auch AWS IAM Identity Center, wenn Sie mit oder anderen AWS Diensten arbeiten, die Konsole, die API oder AWS SDKs verwenden. AWS CLI Alle Daten, die Sie in Tags oder Freiform-Textfelder für Namen eingeben, können für Diagnoseprotokolle verwendet werden.

Verschlüsselung während der Übertragung

IAM Identity Center schützt Daten während der Übertragung zum und vom Service, indem alle Netzwerkdaten automatisch mit dem Verschlüsselungsprotokoll Transport Layer Security (TLS) 1.2 oder TLS 1.3 verschlüsselt werden. Direkte HTTPS-Anfragen, die mit IAM authentifiziert und an das IAM Identity Center APIs, die Identity Store API oder die OIDC API gesendet werden, werden mit dem AWS Signature Version 4-Algorithmus signiert, um eine sichere Verbindung herzustellen.

Datenschutz

Mit IAM Identity Center behalten Sie die Kontrolle über die Daten Ihres Unternehmens. Ihre in IAM Identity Center gespeicherten Benutzer- und Gruppenidentitäten werden nur dann mit anderen AWS Diensten wie AWS verwalteten Anwendungen geteilt, wenn Sie sie mit IAM Identity Center aktivieren und wenn diese Dienste sie benötigen.

Weitere Informationen finden Sie in den häufig gestellten Fragen zum AWS Datenschutz.

Datenaufbewahrung

IAM Identity Center speichert Ihre Daten wie Benutzer- und Gruppenidentitäten sowie Metadaten, bis Sie sie aus dem Dienst löschen. Wenn Sie eine IAM Identity Center-Instanz löschen, werden die darin enthaltenen Daten ebenfalls gelöscht.

Verschlüsselung im Ruhezustand

IAM Identity Center bietet Verschlüsselung zum Schutz von gespeicherten Kundendaten mithilfe der folgenden Schlüsseltypen:

- AWS-eigene Schlüssel (Standardschlüsseltyp) — IAM Identity Center verwendet diese Schlüssel standardmäßig, um Ihre Daten automatisch zu verschlüsseln. Sie können ihre Verwendung nicht einsehen, verwalten, überprüfen oder AWS eigene Schlüssel für andere Zwecke verwenden. IAM Identity Center kümmert sich vollständig um die Schlüsselverwaltung, um die Sicherheit Ihrer Daten zu gewährleisten, ohne dass Sie Maßnahmen ergreifen müssen. Weitere Informationen finden Sie unter AWS -eigene Schlüssel im AWS Key Management Service -Entwicklerhandbuch.
- Vom Kunden verwaltete Schlüssel — In Unternehmensinstanzen von IAM Identity Center können Sie einen symmetrischen, vom Kunden verwalteten Schlüssel für die Verschlüsselung der übrigen Identitätsdaten Ihrer Belegschaft wie Benutzer- und Gruppenattribute wählen. Sie erstellen, besitzen und verwalten diese Verschlüsselungsschlüssel. Da Sie die volle Kontrolle über diese Verschlüsselungsebene haben, können Sie beispielsweise folgende Aufgaben ausführen:
  - Einrichtung und Pflege wichtiger Richtlinien, um den Zugriff auf den Schlüssel nur auf IAM-Prinzipale zu beschränken, die Zugriff benötigen, wie z. B. IAM Identity Center und AWS verwaltete Anwendungen darauf AWS Organizations und deren Administratoren.
  - Einrichtung und Pflege von IAM-Richtlinien für den Zugriff auf den Schlüssel, einschließlich kontoübergreifender Zugriffe
  - Aktivieren und Deaktivieren wichtiger Richtlinien

- Kryptographisches Material mit rotierendem Schlüssel
- Prüfung des Zugriffs auf Ihre Daten, für den ein Schlüsselzugriff erforderlich ist
- Hinzufügen von Tags
- Erstellen von Schlüsselaliasen
- Schlüssel für das Löschen von Schlüsseln planen

Informationen zur Implementierung eines vom Kunden verwalteten KMS-Schlüssels in IAM Identity Center finden Sie unterImplementierung von vom Kunden verwalteten KMS-Schlüsseln in AWS IAM Identity Center. Weitere Informationen zu vom Kunden verwalteten Schlüsseln finden Sie im AWS Key Management Service Entwicklerhandbuch unter Vom Kunden verwaltete Schlüssel.

> **Note**
>
> IAM Identity Center aktiviert automatisch die Verschlüsselung im Ruhezustand mithilfe AWS eigener KMS-Schlüssel, um Kundendaten kostenlos zu schützen. Bei Verwendung eines vom Kunden verwalteten Schlüssels fallen jedoch AWS KMS Gebühren an. Weitere Informationen zur Preisgestaltung finden Sie unter AWS Key Management Service Preisgestaltung.

Überlegungen zur Implementierung von vom Kunden verwalteten Schlüsseln:

- Ausnahme für bestehende Sitzungen: Die Verschlüsselung im Ruhezustand mit einem vom Kunden verwalteten Schlüssel gilt auch für Personalidentitätsdaten wie Benutzer- und Gruppenattribute, die vorübergehend in Benutzersitzungen gespeichert werden. Wenn Sie einen vom Kunden verwalteten Schlüssel in IAM Identity Center konfigurieren, wird der vom Kunden verwaltete Schlüssel verwendet, um Personalidentitätsdaten in neuen Sitzungen zu verschlüsseln. In Sitzungen, die vor der Veröffentlichung dieser Funktion initiiert wurden, bleiben Personalidentitätsdaten standardmäßig verschlüsselt, AWS-eigene Schlüssel bis die Sitzung abläuft (maximal 90 Tage) oder beendet wird. Zu diesem Zeitpunkt werden diese Daten automatisch gelöscht.
- Dedizierte Schlüssel: Wir empfehlen, für jede IAM Identity Center-Instanz einen neuen dedizierten, vom Kunden verwalteten KMS-Schlüssel zu erstellen, anstatt einen vorhandenen Schlüssel wiederzuverwenden. Dieser Ansatz sorgt für eine klarere Aufgabentrennung, vereinfacht die Verwaltung der Zugriffskontrolle und macht die Sicherheitsüberprüfung einfacher. Ein eigener Schlüssel reduziert auch das Risiko, da die Auswirkungen wichtiger Änderungen auf eine einzelne IAM Identity Center-Instanz begrenzt werden.

> **Note**
>
> IAM Identity Center verwendet Umschlagverschlüsselung bei der Verschlüsselung der Identitätsdaten Ihrer Belegschaft. Ihr KMS-Schlüssel spielt die Rolle eines Wrapping-Schlüssels, der den Datenschlüssel verschlüsselt, der tatsächlich zur Verschlüsselung der Daten verwendet wird.

Weitere Informationen zu AWS KMS finden Sie unter Was ist der AWS Schlüsselverwaltungsdienst?

IAM Identity Center-Verschlüsselungskontext

Ein Verschlüsselungskontext ist ein optionaler Satz nicht geheimer Schlüssel-Wert-Paare, die zusätzliche kontextbezogene Informationen zu den Daten enthalten. AWS KMS verwendet den Verschlüsselungskontext als zusätzliche authentifizierte Daten, um die authentifizierte Verschlüsselung zu unterstützen. Wenn Sie einen Verschlüsselungskontext in eine Anforderung zum Verschlüsseln von Daten einbeziehen, wird der Verschlüsselungskontext AWS KMS an die verschlüsselten Daten gebunden. Zur Entschlüsselung von Daten müssen Sie denselben Verschlüsselungskontext in der Anfrage übergeben. Weitere Informationen zum Verschlüsselungskontext finden Sie im AWS KMS Entwicklerhandbuch.

IAM Identity Center verwendet Verschlüsselungskontextschlüssel aus den folgenden Quellen: aws:sso:instance-arn, aws:identitystore:identitystore-arn und. tenant-key-id Beispielsweise kann der folgende Verschlüsselungskontext in API-Vorgängen vorkommen, die von der IAM Identity Center API aufgerufen werden. AWS KMS

```
"encryptionContext": {
    "tenant-key-id": "ssoins-1234567890abcdef",
    "aws:sso:instance-arn": "arn:aws:sso:::instance/ssoins-1234567890abcdef"
}
```

Der folgende Verschlüsselungskontext kann in AWS KMS API-Vorgängen vorkommen, die von der Identity Store API aufgerufen werden.

```
"encryptionContext": {
    "tenant-key-id": "12345678-1234-1234-1234-123456789012",
    "aws:identitystore:identitystore-arn":
 "arn:aws:identitystore::123456789012:identitystore/d-1234567890"
```

```
}
```

Verwendung des Verschlüsselungskontextes zur Steuerung des Zugriffs auf den vom Kunden verwalteten Schlüssel

Sie können den Verschlüsselungskontext in Schlüsselrichtlinien und IAM-Richtlinien als Bedingungen verwenden, um den Zugriff auf Ihren symmetrischen, vom Kunden verwalteten Schlüssel zu kontrollieren. Einige der wichtigsten Richtlinienvorlagen in der Wichtige KMS-Richtlinienerklärungen für Fortgeschrittene enthalten solche Bedingungen, um sicherzustellen, dass der Schlüssel nur mit einer bestimmten IAM Identity Center-Instanz verwendet wird.

Überwachung Ihrer Verschlüsselungsschlüssel für IAM Identity Center

Wenn Sie einen vom Kunden verwalteten KMS-Schlüssel mit Ihrer IAM Identity Center-Instance verwenden, können Sie AWS CloudTrailoder Amazon CloudWatch Logs verwenden, um Anfragen zu verfolgen, an die IAM Identity Center sendet. AWS KMS Die KMS-API-Operationen, die IAM Identity Center aufruft, sind unter aufgeführt. Schritt 2: Bereiten Sie die wichtigsten Richtlinienerklärungen für KMS vor CloudTrail Ereignisse für diese API-Operationen enthalten den Verschlüsselungskontext, der es Ihnen ermöglicht, AWS KMS API-Operationen zu überwachen, die von Ihrer IAM Identity Center-Instanz aufgerufen werden, um auf Daten zuzugreifen, die mit Ihrem vom Kunden verwalteten Schlüssel verschlüsselt wurden.

Beispiel für einen Verschlüsselungskontext im CloudTrail Fall eines AWS KMS API-Vorgangs:

```
{
"requestParameters": {
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "encryptionContext": {
            "aws:sso:instance-arn": "arn:aws:sso:::instance/ssoins-xxxxxxxxxxxxxxxx",
            "tenant-key-id": "ssoins-xxxxxxxxxxxxxxxx"
        }
    }
}
```

AWS Speicherung, Verschlüsselung und Löschung von IAM Identity Center-Identitätsattributen durch verwaltete Anwendungen

Einige AWS verwaltete Anwendungen, die Sie bereitstellen AWS IAM Identity Center, wie AWS Systems Manager und Amazon CodeCatalyst, speichern bestimmte Benutzer- und Gruppenattribute

aus IAM Identity Center in ihrem eigenen Datenspeicher. Die Verschlüsselung im Ruhezustand mit einem vom Kunden verwalteten KMS-Schlüssel in IAM Identity Center erstreckt sich nicht auf die IAM Identity Center-Benutzer- und Gruppenattribute, die in AWS verwalteten Anwendungen gespeichert sind. AWS verwaltete Anwendungen unterstützen verschiedene Verschlüsselungsmethoden für die von ihnen gespeicherten Daten. Und wenn Sie Benutzer- und Gruppenattribute in IAM Identity Center löschen, speichern diese AWS verwalteten Anwendungen diese Informationen möglicherweise auch nach dem Löschen in IAM Identity Center weiter. Informationen zur Verschlüsselung und Sicherheit der in den Anwendungen gespeicherten Daten finden Sie im Benutzerhandbuch Ihrer AWS verwalteten Anwendungen.

Implementierung von vom Kunden verwalteten KMS-Schlüsseln in AWS IAM Identity Center

Kundenverwaltete Schlüssel sind AWS Schlüssel des Key Management Service, die Sie selbst erstellen, besitzen und verwalten. Gehen Sie wie folgt vor, um einen vom Kunden verwalteten KMS-Schlüssel für die Verschlüsselung im Ruhezustand in AWS IAM Identity Center zu implementieren:

> **Important**
>
> Einige AWS verwaltete Anwendungen können nicht mit AWS IAM Identity Center verwendet werden, das mit einem vom Kunden verwalteten KMS-Schlüssel konfiguriert ist. Siehe AWS verwaltete Anwendungen, die Sie mit IAM Identity Center verwenden können.

1. Schritt 1: Identifizieren Sie Anwendungsfälle für Ihr Unternehmen- Um die richtigen Berechtigungen für die Verwendung des KMS-Schlüssels zu definieren, müssen Sie die relevanten Anwendungsfälle in Ihrem Unternehmen identifizieren. Die KMS-Schlüsselberechtigungen bestehen aus KMS-Schlüsselrichtlinienerklärungen und identitätsbasierten Richtlinien, die zusammenwirken, sodass die entsprechenden IAM-Prinzipale den KMS-Schlüssel für ihre spezifischen Anwendungsfälle verwenden können.
2. Schritt 2: Bereiten Sie die wichtigsten Richtlinienerklärungen für KMS vor- Wählen Sie auf der Grundlage der in Schritt 1 identifizierten Anwendungsfälle die entsprechenden Vorlagen für KMS-Schlüsselrichtlinienerklärungen aus und geben Sie die erforderlichen Kennungen und IAM-Prinzipalnamen ein. Beginnen Sie mit den grundlegenden KMS-Richtlinienaussagen und verfeinern Sie sie, falls Ihre Sicherheitsrichtlinien dies erfordern, wie unter Erweiterte KMS-Richtlinienerklärungen beschrieben.

3. Schritt 3: Erstellen Sie einen vom Kunden verwalteten KMS-Schlüssel- Erstellen Sie in KMS einen AWS KMS-Schlüssel, der die Anforderungen von IAM Identity Center erfüllt, und fügen Sie die in Schritt 2 erstellten KMS-Schlüsselrichtlinienanweisungen zur KMS-Schlüsselrichtlinie hinzu.
4. Schritt 4: Konfigurieren Sie IAM-Richtlinien für die kontoübergreifende Verwendung des KMS-Schlüssels- Wählen Sie auf der Grundlage der in Schritt 1 identifizierten Anwendungsfälle entsprechende Vorlagen für IAM-Richtlinienerklärungen aus und bereiten Sie sie für die Verwendung vor, indem Sie den Schlüssel-ARN ARN. Erlauben Sie dann den IAM-Prinzipalen für jeden spezifischen Anwendungsfall, den KMS-Schlüssel kontenübergreifend zu verwenden, indem Sie die vorbereiteten IAM-Richtlinienerklärungen zu den IAM-Richtlinien der Principals hinzufügen.
5. Schritt 5: Konfigurieren Sie den KMS-Schlüssel im IAM Identity Center- Aktivieren Sie den vom Kunden verwalteten KMS-Schlüssel in Ihrer IAM Identity Center-Instanz, um ihn für die Verschlüsselung im Ruhezustand zu verwenden.

> **Important**
>
> Bevor Sie mit diesem Schritt fortfahren, überprüfen Sie gründlich alle in den vorherigen Schritten konfigurierten KMS-Schlüsselberechtigungen. Sobald der Vorgang abgeschlossen ist, verwendet IAM Identity Center den KMS-Schlüssel für die Verschlüsselung im Ruhezustand.

Schritt 1: Identifizieren Sie Anwendungsfälle für Ihr Unternehmen

Bevor Sie Ihren vom Kunden verwalteten KMS-Schlüssel erstellen und konfigurieren, identifizieren Sie Ihre Anwendungsfälle und bereiten Sie die erforderlichen KMS-Schlüsselberechtigungen vor. Weitere Informationen zur AWS KMS-Schlüsselrichtlinie finden Sie im KMS-Entwicklerhandbuch.

IAM-Prinzipale, die den IAM Identity Center-Dienst APIs aufrufen, benötigen Berechtigungen. Ein delegierter Administrator kann beispielsweise APIs über eine Berechtigungssatzrichtlinie autorisiert werden, diese zu verwenden. Wenn IAM Identity Center mit einem vom Kunden verwalteten Schlüssel konfiguriert ist, müssen IAM-Prinzipale auch über die Berechtigungen verfügen, die KMS-API über den IAM Identity Center-Dienst zu verwenden. APIs Sie definieren diese KMS-API-Berechtigungen an zwei Stellen: in der KMS-Schlüsselrichtlinie und in den IAM-Richtlinien, die den IAM-Prinzipalen zugeordnet sind.

Die KMS-Schlüsselberechtigungen bestehen aus:

1. KMS-Schlüsselrichtlinienanweisungen, die Sie für den KMS-Schlüssel bei seiner Erstellung in angebenSchritt 3: Erstellen Sie einen vom Kunden verwalteten KMS-Schlüssel.
2. IAM-Richtlinienanweisungen für IAM-Prinzipale, die Sie Schritt 4: Konfigurieren Sie IAM-Richtlinien für die kontoübergreifende Verwendung des KMS-Schlüssels nach der Erstellung des KMS-Schlüssels angeben.

In der folgenden Tabelle sind die relevanten Anwendungsfälle und IAM-Prinzipale aufgeführt, für die Berechtigungen zur Verwendung Ihres KMS-Schlüssels erforderlich sind.

Anwendungsfall	IAM-Prinzipale, die Berechtigungen zur Verwendung des KMS-Schlüssels benötigen	Erforderlich/optional
Verwendung von AWS IAM Identity Center	• Administratoren von AWS IAM Identity Center • Der IAM Identity Center-Dienst und der zugehörige Identity Store-Dienst	Erforderlich
Verwendung AWS verwalteter Anwendungen mit IAM Identity Center	• Administratoren AWS verwalteter Anwendungen • AWS verwaltete Anwendungen • Dienstrollen, von denen AWS verwaltete Anwendungen annehmen, dass sie den IAM Identity Center-Dienst aufrufen APIs	Optional
Verwendung von AWS Control Tower auf der AWS IAM Identity Center-Instanz, die sie aktiviert hat	• AWS Control Tower Administratoren	Optional
SSO für Amazon EC2 Windows-Instances mit AWS IAM Identity Center	• IAM-Principals, die autorisiert sind, SSO für Amazon EC2 Windows-Instances durchzuführen	Optional

Anwendungsfall	IAM-Prinzipale, die Berechtigungen zur Verwendung des KMS-Schlüssels benötigen	Erforderlich/optional
Jeder andere Anwendungsfall, bei dem der IAM Identity Center-Service APIs mit IAM-Prinzipalen aufgerufen wird, wie z. B. vom Kunden verwaltete Anwendungen, Workflows zur Bereitstellung von Berechtigungssätzen oder Funktionen AWS Lambda	• IAM-Prinzipale, die von diesen Workflows verwendet werden, um den IAM Identity Center-Dienst aufzurufen APIs	Optional

> **Note**
>
> Für mehrere in der Tabelle aufgeführte IAM-Prinzipale sind KMS-API-Berechtigungen erforderlich. AWS Um Ihre Benutzer- und Gruppendaten in IAM Identity Center zu schützen, rufen jedoch nur die Dienste IAM Identity Center und Identity Store die KMS-API direkt auf. AWS

Schritt 2: Bereiten Sie die wichtigsten Richtlinienerklärungen für KMS vor

Nachdem Sie die für Ihr Unternehmen relevanten Anwendungsfälle identifiziert haben, können Sie die entsprechenden wichtigsten KMS-Richtlinienerklärungen vorbereiten.

1. Wählen Sie die wichtigsten KMS-Richtlinienerklärungen aus, die den Anwendungsfällen für Ihre Organisation entsprechen. Beginnen Sie mit den grundlegenden Richtlinienvorlagen. Wenn Sie spezifischere Richtlinien benötigen, die auf Ihren Sicherheitsanforderungen basieren, können Sie die Richtlinienerklärungen anhand der Beispiele unter ändernWichtige KMS-Richtlinienerklärungen für Fortgeschrittene. Hinweise zu dieser Entscheidung finden Sie unterÜberlegungen zur Auswahl grundlegender und erweiterter KMS-Richtlinien. Darüber hinaus Grundlegende KMS-Schlüssel- und IAM-Richtlinienerklärungen enthält jeder Basisabschnitt entsprechende Überlegungen.
2. Kopieren Sie die entsprechenden Richtlinien in einen Editor und fügen Sie die erforderlichen Kennungen und IAM-Prinzipalnamen in die wichtigsten KMS-Richtlinienerklärungen ein. Hilfe

bei der Suche nach den Werten der referenzierten Bezeichner finden Sie unter. Finden Sie die erforderlichen Kennungen

Im Folgenden finden Sie grundlegende Richtlinienvorlagen für jeden Anwendungsfall. Für die Verwendung eines KMS-Schlüssels ist nur der erste Satz von Berechtigungen für AWS IAM Identity Center erforderlich. Wir empfehlen Ihnen, die entsprechenden Unterabschnitte zu lesen, um weitere anwendungsfallspezifische Informationen zu erhalten.

- Grundlegende KMS-Richtlinienerklärungen für die Verwendung von IAM Identity Center (erforderlich)
- Grundlegende KMS-Schlüssel- und IAM-Richtlinienerklärungen für die Verwendung verwalteter Anwendungen AWS
- Grundlegende KMS-Schlüsselaussage für die Verwendung von AWS Control Tower
- Grundlegende KMS-Schlüssel- und IAM-Richtlinienerklärungen für die Verwendung von IAM Identity Center für Amazon Elastic Compute Cloud Windows-Instances
- Grundlegende KMS-Schlüssel- und IAM-Richtlinienerklärungen für die Verwendung benutzerdefinierter Workflows mit IAM Identity Center

Important

Seien Sie vorsichtig, wenn Sie KMS-Schlüsselrichtlinien für Schlüssel ändern, die bereits von IAM Identity Center verwendet werden. IAM Identity Center validiert zwar die Verschlüsselungs- und Entschlüsselungsberechtigungen bei der ersten Konfiguration eines KMS-Schlüssels, kann jedoch nachfolgende Richtlinienänderungen nicht verifizieren. Wenn Sie versehentlich die erforderlichen Berechtigungen entfernen, kann dies den normalen Betrieb Ihres IAM Identity Center stören. Anleitungen zur Behebung häufiger Fehler im Zusammenhang mit vom Kunden verwalteten Schlüsseln in IAM Identity Center finden Sie unter. Problembehandlung bei vom Kunden verwalteten Schlüsseln in AWS IAM Identity Center

Note

Für das IAM Identity Center und der zugehörige Identity Store sind Service-Level-Berechtigungen erforderlich, um Ihren vom Kunden verwalteten KMS-Schlüssel verwenden zu können. Diese Anforderung gilt auch für AWS verwaltete Anwendungen,

die den IAM Identity Center-Dienst APIs mithilfe von Dienstanmeldedaten aufrufen. In anderen Anwendungsfällen, in denen der IAM Identity Center-Dienst APIs mit Forward-Access-Sitzungen aufgerufen wird, benötigt nur der initiierende IAM-Prinzipal (z. B. ein Administrator) KMS-Schlüsselberechtigungen. Insbesondere Endbenutzer, die das AWS Zugriffsportal und AWS verwaltete Anwendungen verwenden, benötigen keine direkten KMS-Schlüsselberechtigungen, da sie über die jeweiligen Dienste erteilt werden.

Schritt 3: Erstellen Sie einen vom Kunden verwalteten KMS-Schlüssel

Sie können mit der AWS Management Console oder dem AWS KMS APIs einen vom Kunden verwalteten Schlüssel erstellen. Fügen Sie bei der Erstellung des Schlüssels die in Schritt 2 erstellten KMS-Schlüsselrichtlinienanweisungen zur KMS-Schlüsselrichtlinie hinzu. Ausführliche Anweisungen, einschließlich Anleitungen zur standardmäßigen KMS-Schlüsselrichtlinie, finden Sie im AWS Key Management Service Developer Guide.

Der Schlüssel muss die folgenden Anforderungen erfüllen:

- Der KMS-Schlüssel muss sich in derselben AWS Region befinden wie die IAM Identity Center-Instanz
- Sie können entweder einen Schlüssel für mehrere Regionen oder einen Schlüssel für eine einzelne Region wählen. Um zukunftskompatibel mit Ihren future Anwendungsfällen in mehreren AWS Regionen zu bleiben, empfehlen wir, einen Schlüssel für mehrere Regionen zu wählen
- Der KMS-Schlüssel muss ein symmetrischer Schlüssel sein, der für die Verwendung „Verschlüsseln und Entschlüsseln“ konfiguriert ist
- Der KMS-Schlüssel muss sich in demselben AWS Organizations Verwaltungskonto befinden wie die Organisationsinstanz von IAM Identity Center

Schritt 4: Konfigurieren Sie IAM-Richtlinien für die kontoübergreifende Verwendung des KMS-Schlüssels

Jeder IAM-Prinzipal, der den IAM Identity Center-Dienst APIs von einem anderen AWS Konto aus verwendet, z. B. delegierte IAM Identity Center-Administratoren, benötigt ebenfalls eine IAM-Richtlinienerklärung, die die Verwendung des KMS-Schlüssels über diese Konten ermöglicht. APIs

Für jeden in Schritt 1 identifizierten Anwendungsfall gilt Folgendes:

1. Suchen Sie die entsprechenden Vorlagen für IAM-Richtlinienanweisungen unter Basis-KMS-Schlüssel und IAM-Richtlinienanweisungen.
2. Kopieren Sie die Vorlagen in einen Editor und geben Sie den Schlüssel ARN ein, der jetzt nach der Erstellung des KMS-Schlüssels in Schritt 3 verfügbar ist. Hilfe bei der Suche nach dem ARN-Schlüsselwert finden Sie unterFinden Sie die erforderlichen Kennungen.
3. Suchen Sie in der AWS-Managementkonsole nach der IAM-Richtlinie des IAM-Prinzipals, der dem Anwendungsfall zugeordnet ist. Der Speicherort dieser Richtlinie hängt vom Anwendungsfall und davon ab, wie der Zugriff gewährt wird.
   - Für den Zugriff, der direkt in IAM gewährt wird, können Sie in der IAM-Konsole nach IAM-Prinzipalen suchen, z. B. nach IAM-Rollen.
   - Für den Zugriff, der über IAM Identity Center gewährt wird, finden Sie den entsprechenden Berechtigungssatz in der IAM Identity Center-Konsole.
4. Fügen Sie die anwendungsfallspezifischen IAM-Richtlinienanweisungen zur IAM-Rolle hinzu und speichern Sie die Änderung.

> **Note**
>
> Bei den hier beschriebenen IAM-Richtlinien handelt es sich um identitätsbasierte Richtlinien. Solche Richtlinien können zwar IAM-Benutzern, -Gruppen und -Rollen zugewiesen werden, wir empfehlen jedoch, wenn möglich, IAM-Rollen zu verwenden. Weitere Informationen zu IAM-Rollen im Vergleich zu IAM-Benutzern finden Sie im IAM-Benutzerhandbuch.

Zusätzliche Konfiguration in einigen verwalteten Anwendungen AWS

Bei einigen AWS verwalteten Anwendungen müssen Sie eine Servicerolle konfigurieren, damit die Anwendungen den IAM Identity Center-Dienst APIs nutzen können. Wenn Ihr Unternehmen AWS verwaltete Anwendungen mit IAM Identity Center verwendet, führen Sie für jede bereitgestellte Anwendung die folgenden Schritte aus:

1. Überprüfen Sie im Benutzerhandbuch der Anwendung, ob die Berechtigungen aktualisiert wurden und nun auch Berechtigungen für KMS-Schlüssel für die Verwendung der Anwendung mit IAM Identity Center enthalten.
2. Falls ja, aktualisieren Sie die Berechtigungen gemäß den Anweisungen im Benutzerhandbuch der Anwendung, um Störungen des Anwendungsbetriebs zu vermeiden.

> **Note**
>
> Wenn Sie sich nicht sicher sind, ob eine AWS verwaltete Anwendung diese Berechtigungen verwendet, empfehlen wir Ihnen, die Benutzerhandbücher aller bereitgestellten AWS verwalteten Anwendungen zu lesen. Sie müssen diese Konfiguration nur einmal für jede Anwendung durchführen, für die die Konfiguration erforderlich ist.

Schritt 5: Konfigurieren Sie den KMS-Schlüssel im IAM Identity Center

> **Important**
>
> Bevor Sie mit diesem Schritt fortfahren:
>
> - Stellen Sie sicher, dass Ihre AWS verwalteten Anwendungen mit vom Kunden verwalteten KMS-Schlüsseln kompatibel sind. Eine Liste kompatibler Anwendungen finden Sie unter AWS Verwaltete Anwendungen, die Sie mit IAM Identity Center verwenden können. Wenn Sie inkompatible Anwendungen haben, fahren Sie nicht fort.
> - Konfigurieren Sie die erforderlichen Berechtigungen für die Verwendung des KMS-Schlüssels. Ohne die entsprechenden Berechtigungen kann dieser Schritt fehlschlagen oder die IAM Identity Center-Verwaltung, die Verwendung AWS verwalteter Anwendungen und andere Anwendungsfälle, für die KMS-Schlüsselberechtigungen erforderlich sind, unterbrechen. Weitere Informationen finden Sie unter Schritt 1: Identifizieren Sie Anwendungsfälle für Ihr Unternehmen.
> - Stellen Sie sicher, dass Berechtigungen für AWS verwaltete Anwendungen und vom Kunden verwaltete Anwendungen, die den IAM Identity Center-Dienst APIs mit IAM-Rollen aufrufen, auch die Verwendung des KMS-Schlüssels über den IAM Identity Center-Dienst zulassen. APIs Bei einigen AWS verwalteten Anwendungen müssen Sie Berechtigungen, wie z. B. eine Servicerolle, für deren Verwendung konfigurieren. APIs Prüfen Sie im Benutzerhandbuch jeder bereitgestellten AWS verwalteten Anwendung, ob Sie bestimmte KMS-Schlüsselberechtigungen hinzufügen müssen.

Geben Sie einen KMS-Schlüssel an, wenn Sie eine neue Organisationsinstanz von IAM Identity Center aktivieren

Wenn Sie eine neue Organisationsinstanz von IAM Identity Center aktivieren, können Sie bei der Einrichtung einen vom Kunden verwalteten KMS-Schlüssel angeben. Dadurch wird sichergestellt, dass die Instanz Ihren Schlüssel von Anfang an für die Verschlüsselung im Ruhezustand verwendet. Bevor Sie beginnen, finden Sie weitere Informationen unterÜberlegungen zu vom Kunden verwalteten KMS-Schlüsseln und erweiterten KMS-Schlüsselrichtlinien.

1. Erweitern Sie auf der Seite „IAM Identity Center aktivieren“ den Abschnitt Verschlüsselung im Ruhezustand.
2. Wählen Sie Manage Encryption (Verschlüsselung verwalten).
3. Wählen Sie Vom Kunden verwalteter Schlüssel aus.
4. Führen Sie für den KMS-Schlüssel einen der folgenden Schritte aus:

    a. Wählen Sie Aus Ihren KMS-Schlüsseln auswählen und wählen Sie den Schlüssel, den Sie erstellt haben, aus der Dropdownliste aus.

    b. Wählen Sie Enter KMS key ARN und geben Sie den vollständigen ARN Ihres Schlüssels ein.
5. Wählen Sie Speichern.
6. Wählen Sie Aktivieren, um die Einrichtung abzuschließen.

Weitere Informationen finden Sie unter IAM Identity Center aktivieren.

Ändern Sie die Schlüsselkonfiguration für eine bestehende Organisationsinstanz von IAM Identity Center

Sie können Ihren vom Kunden verwalteten KMS-Schlüssel jederzeit in einen anderen Schlüssel ändern oder AWS zu einem eigenen Schlüssel wechseln.

Console

Um die Konfiguration Ihres KMS-Schlüssels zu ändern

1. Öffnen Sie die IAM Identity Center-Konsole unter https://console.aws.amazon.com/singlesignon/.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie die Registerkarte Zusätzliche Einstellungen.

4. Wählen Sie Verschlüsselung verwalten aus.
5. Wählen Sie eine der folgenden Optionen aus:

   a. Vom Kunden verwalteter Schlüssel — Wählen Sie einen anderen vom Kunden verwalteten Schlüssel aus der Dropdownliste aus oder geben Sie einen neuen Schlüssel-ARN ein.

   b. AWS Eigener Schlüssel — Wechseln Sie zur Standardverschlüsselungsoption.
6. Wählen Sie Speichern.

AWS CLI

Um eine bestehende Organisationsinstanz von IAM Identity Center so zu ändern, dass sie den vom Kunden verwalteten KMS-Schlüssel verwendet

```
aws sso-admin update-instance \
    --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \
    --encryption-configuration \
        KeyType=CUSTOMER_MANAGED_KEY,KmsKeyArn=arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Um eine bestehende Organisationsinstanz von IAM Identity Center so zu ändern, dass sie einen eigenen Schlüssel verwendet AWS

```
aws sso-admin update-instance \
    --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \
    --encryption-configuration KeyType=AWS_OWNED_KMS_KEY
```

Vom Kunden verwaltete wichtige Überlegungen

- Die Aktualisierung der KMS-Schlüsselkonfiguration für den Betrieb von IAM Identity Center hat keine Auswirkungen auf aktive Benutzersitzungen in Ihrem IAM Identity Center. Während dieses Vorgangs können Sie das AWS Zugriffsportal, die IAM Identity Center-Konsole und den IAM Identity Center-Dienst APIs weiterhin verwenden.
- Wenn Sie zu einem neuen KMS-Schlüssel wechseln, überprüft IAM Identity Center, ob der Schlüssel erfolgreich für die Verschlüsselung und Entschlüsselung verwendet werden kann. Wenn Sie bei der Einrichtung der Schlüssel- oder IAM-Richtlinie einen Fehler gemacht haben, zeigt

die Konsole eine erklärende Fehlermeldung an, und der vorherige KMS-Schlüssel wird weiterhin verwendet.
- Die standardmäßige jährliche KMS-Schlüsselrotation erfolgt automatisch. Informationen zu Themen wie Schlüsselrotation, Überwachung von AWS KMS Schlüsseln und Steuerung des Zugriffs auf das Löschen von Schlüsseln finden Sie im AWS KMS Entwicklerhandbuch.

> **Important**
>
> Wenn der von Ihrer IAM Identity Center-Instanz verwendete, vom Kunden verwaltete KMS-Schlüssel gelöscht, deaktiviert oder aufgrund einer falschen KMS-Schlüsselrichtlinie nicht zugänglich ist, können Ihre Belegschaftsbenutzer und IAM Identity Center-Administratoren IAM Identity Center nicht verwenden. Der Verlust des Zugriffs kann je nach den Umständen vorübergehend (eine wichtige Richtlinie kann korrigiert werden) oder dauerhaft (ein gelöschter Schlüssel kann nicht wiederhergestellt werden) sein. Wir empfehlen Ihnen, den Zugriff auf kritische Vorgänge wie das Löschen oder Deaktivieren des KMS-Schlüssels zu beschränken. Außerdem empfehlen wir, dass Ihr Unternehmen AWS glasklare Zugriffsverfahren einrichtet, um sicherzustellen, dass Ihre privilegierten Benutzer AWS in dem unwahrscheinlichen Fall, dass auf IAM Identity Center nicht zugegriffen werden kann, darauf zugreifen können.

Finden Sie die erforderlichen Kennungen

Bei der Konfiguration von Berechtigungen für Ihren vom Kunden verwalteten KMS-Schlüssel benötigen Sie spezifische AWS Ressourcen-IDs, um die Vorlagen für Schlüsselrichtlinien und IAM-Richtlinienerklärungen auszufüllen. Fügen Sie die erforderlichen Kennungen (z. B. die Organisations-ID) und die IAM-Prinzipalnamen in die wichtigsten KMS-Richtlinienerklärungen ein.

Im Folgenden finden Sie eine Anleitung zum Auffinden dieser Kennungen in der AWS Management Console.

IAM Identity Center Amazon-Ressourcenname (ARN) und Identitätsspeicher-ARN

Eine IAM Identity Center-Instanz ist eine AWS Ressource mit einem eigenen eindeutigen ARN wie arn:aws:sso: ::instance/ssoins-1234567890abcdef. Der ARN folgt dem Muster, das im Abschnitt IAM Identity Center-Ressourcentypen der Service Authorization Reference dokumentiert ist.

Jeder IAM Identity Center-Instanz ist ein Identity Store zugeordnet, in dem die Benutzer- und Gruppenidentitäten gespeichert werden. Ein Identity Store hat eine eindeutige Kennung namens

Identity Store ID (z. B. d-123456789a). Der ARN folgt dem Muster, das im Abschnitt Identity Store-Ressourcentypen der Service Authorization Reference dokumentiert ist.

Sie finden sowohl die ARN- als auch die Identity Store-ID-Werte auf der Einstellungsseite Ihres IAM Identity Center. Die Identity Store-ID befindet sich auf der Registerkarte Identitätsquelle.

AWS Organizations ID (ID)

Wenn Sie eine Organisations-ID (z. B. o-exampleorg1) in Ihrer Schlüsselrichtlinie angeben möchten, finden Sie ihren Wert auf der Einstellungsseite Ihres IAM Identity Center und der Organisationskonsole. Der ARN folgt dem Muster, das im Abschnitt Ressourcentypen für Organizations der Service Authorization Reference dokumentiert ist.

KMS-Schlüssel ARN

Sie finden den ARN eines KMS-Schlüssels in der AWS KMS Konsole. Wählen Sie links vom Kunden verwaltete Schlüssel aus, klicken Sie auf den Schlüssel, dessen ARN Sie nachschlagen möchten, und Sie werden ihn im Abschnitt Allgemeine Konfiguration sehen. Der ARN folgt dem Muster, das im Abschnitt AWS KMS Ressourcentypen der Service Authorization Reference dokumentiert ist.

Weitere Informationen zu den wichtigsten Richtlinien AWS KMS und zur Problembehandlung bei AWS KMS Berechtigungen finden Sie im AWS Key Management Service Entwicklerhandbuch. Weitere Informationen zu IAM-Richtlinien und ihrer JSON-Darstellung finden Sie im IAM-Benutzerhandbuch.

Grundlegende KMS-Schlüssel- und IAM-Richtlinienerklärungen

Die hier bereitgestellten grundlegenden Richtlinien für KMS-Schlüssel und Identitäten dienen als Grundlage für allgemeine Anforderungen. Wir empfehlen Ihnen außerdem, zu überprüfenWichtige KMS-Richtlinienerklärungen für Fortgeschrittene, ob detailliertere Zugriffskontrollen vorgesehen sind, z. B. sicherzustellen, dass der KMS-Schlüssel nur einer bestimmten IAM Identity Center-Instanz oder verwalteten Anwendung zugänglich ist. AWS Bevor Sie erweiterte KMS-Schlüsselrichtlinienerklärungen verwenden, lesen Sie die. Überlegungen zur Auswahl grundlegender und erweiterter KMS-Richtlinien

Die folgenden Abschnitte enthalten grundlegende Richtlinienaussagen für jeden Anwendungsfall. Kopieren Sie die wichtigsten KMS-Richtlinienaussagen, die Ihren Anwendungsfällen entsprechen, und kehren Sie dann zu zurückSchritt 2: Bereiten Sie die wichtigsten Richtlinienerklärungen für KMS vor.

- Grundlegende KMS-Richtlinienerklärungen für die Verwendung von IAM Identity Center (erforderlich)
- Grundlegende KMS-Schlüssel- und IAM-Richtlinienerklärungen für die Verwendung verwalteter Anwendungen AWS
- Grundlegende KMS-Schlüsselaussage für die Verwendung von AWS Control Tower
- Grundlegende KMS-Schlüssel- und IAM-Richtlinienerklärungen für die Verwendung von IAM Identity Center für Amazon Elastic Compute Cloud Windows-Instances
- Grundlegende KMS-Schlüssel- und IAM-Richtlinienerklärungen für die Verwendung benutzerdefinierter Workflows mit IAM Identity Center

Grundlegende KMS-Richtlinienerklärungen für die Verwendung von IAM Identity Center (erforderlich)

Verwenden Sie die folgende Vorlage für wichtige KMS-Richtlinien, Schritt 2: Bereiten Sie die wichtigsten Richtlinienerklärungen für KMS vor um IAM Identity Center, dem zugehörigen Identity Store und IAM Identity Center-Administratoren die Verwendung des KMS-Schlüssels zu ermöglichen.

- Geben Sie im Element Principal für Administratorrichtlinienanweisungen die AWS Kontenprinzipale der Administratorkonten des IAM Identity Center an, d. h. das AWS Organisationsverwaltungskonto und das delegierte Administratorkonto, und verwenden Sie dabei das Format „arn:aws:iam: :111122223333:root“.
- Ersetzen Sie im Element das Beispiel durch die IAM-Rollen der IAM Identity Center-Administratoren. PrincipalArn ARNs

  Sie können entweder angeben:

  - Spezifischer ARN für IAM-Rollen:

    ```
    "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/ap-southeast-2/AWSReservedSSO_permsetname_12345678"
    ```

  - Platzhaltermuster (empfohlen):

    ```
    "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/ap-southeast-2/AWSReservedSSO_permsetname_*"
    ```

  Die Verwendung des Platzhalters (*) verhindert den Verlust des Zugriffs, wenn der Berechtigungssatz gelöscht und neu erstellt wird, da Identity Center neue eindeutige Identifikatoren

für neu erstellte Berechtigungssätze generiert. Eine Beispielimplementierung finden Sie unter. Beispiel für eine benutzerdefinierte Vertrauensrichtlinie

- Geben Sie im SourceAccount Element die IAM Identity Center-Konto-ID an.
- Identity Store hat seinen eigenen Dienstprinzipal`identitystore.amazonaws.com`, dem die Verwendung des KMS-Schlüssels gestattet sein muss.
- Diese Richtlinienerklärungen ermöglichen es Ihren IAM Identity Center-Instanzen in einem bestimmten AWS Konto, den KMS-Schlüssel zu verwenden. Informationen zum Einschränken des Zugriffs auf eine bestimmte IAM Identity Center-Instanz finden Sie unter. Wichtige KMS-Richtlinienerklärungen für Fortgeschrittene Sie können für jedes AWS Konto nur eine IAM Identity Center-Instanz haben.

Die wichtigsten Richtlinienerklärungen von KMS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowIAMIdentityCenterAdminToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:root",
          "arn:aws:iam::444455556666:root"
        ]
      },
      "Action": [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_AdminPermissionSet_*",
            "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_DelegatedAdminSet_*"
          ]
        },
```

```
        "StringLike": {
          "kms:EncryptionContext:aws:sso:instance-arn": "*",
          "kms:ViaService": "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowIAMIdentityCenterAdminToUseTheKMSKeyViaIdentityStore",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:root",
          "arn:aws:iam::444455556666:root"
        ]
      },
      "Action": [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_AdminPermissionSet_*",
            "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_DelegatedAdminSet_*"
          ]
        },
        "StringLike": {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*",
          "kms:ViaService": "identitystore.*.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowIAMIdentityCenterAdminToDescribeTheKMSKey",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:root",
          "arn:aws:iam::444455556666:root"
        ]
```

```
      },
      "Action": "kms:DescribeKey",
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_AdminPermissionSet_*",
            "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_DelegatedAdminSet_*"
          ]
        }
      }
    },
    {
      "Sid": "AllowIAMIdentityCenterToUseTheKMSKey",
      "Effect": "Allow",
      "Principal": {
        "Service": "sso.amazonaws.com"
      },
      "Action": [
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws:sso:instance-arn": "*"
        },
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        }
      }
    },
    {
      "Sid": "AllowIAMIdentityStoreToUseTheKMSKey",
      "Effect": "Allow",
      "Principal": {
        "Service": "identitystore.amazonaws.com"
      },
      "Action": [
        "kms:Decrypt",
```

```
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
        },
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        }
      }
    },
    {
      "Sid": "AllowIAMIdentityCenterAndIdentityStoreToDescribeKMSKey",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "identitystore.amazonaws.com",
          "sso.amazonaws.com"
        ]
      },
      "Action": "kms:DescribeKey",
      "Resource": "*"
    }
  ]
}
```

Verwenden Sie die folgende Vorlage für IAM-Richtlinienanweisungen, the section called “Schritt 4: Konfigurieren Sie IAM-Richtlinien” um IAM Identity Center-Administratoren die Verwendung des KMS-Schlüssels zu ermöglichen.

- Ersetzen Sie den Beispielschlüssel-ARN im `Resource` Element durch Ihren tatsächlichen KMS-Schlüssel-ARN. Hilfe bei der Suche nach den Werten der referenzierten Bezeichner finden Sie unterFinden Sie die erforderlichen Kennungen.
- Diese IAM-Richtlinienanweisungen gewähren KMS-Schlüsselzugriff auf den IAM-Prinzipal, schränken jedoch nicht ein, welcher AWS Dienst die Anfrage stellen kann. Die KMS-Schlüsselrichtlinie sieht in der Regel diese Diensteinschränkungen vor. Sie können dieser IAM-Richtlinie jedoch einen Verschlüsselungskontext hinzufügen, um die Nutzung auf eine

bestimmte Identity Center-Instanz zu beschränken. Einzelheiten finden Sie unter. Wichtige KMS-Richtlinienerklärungen für Fortgeschrittene

Für delegierte Administratoren von IAM Identity Center sind IAM-Richtlinienerklärungen erforderlich

```
{
  "Version": "2012-10-17",
  "Statement": [{
      "Sid": "IAMPolicyToAllowIAMIdentityCenterAdminToUseKMSkey",
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:DescribeKey"
      ],
      "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    {
      "Sid": "IAMPolicyToAllowIAMIdentityCenterAdminToListKeyAliases",
      "Effect": "Allow",
      "Action": "kms:ListAliases",
      "Resource": "*"
    }
  ]
}
```

Grundlegende KMS-Schlüssel- und IAM-Richtlinienerklärungen für die Verwendung verwalteter Anwendungen AWS

> **Note**
>
> Einige AWS verwaltete Anwendungen können nicht verwendet werden, wenn IAM Identity Center mit einem vom Kunden verwalteten KMS-Schlüssel konfiguriert ist. Weitere Informationen finden Sie unter AWS Verwaltete Anwendungen, die mit IAM Identity Center funktionieren.

Verwenden Sie die folgende Vorlage für eine KMS-SchlüsselrichtlinieSchritt 2: Bereiten Sie die wichtigsten Richtlinienerklärungen für KMS vor, um sowohl AWS verwalteten Anwendungen als auch ihren Administratoren die Verwendung des KMS-Schlüssels zu ermöglichen.

- Geben Sie Ihre AWS Organizations ID in die PrincipalOrg ID und die SourceOrgId Bedingungen ein. Hilfe bei der Suche nach den Werten der referenzierten Identifikatoren finden Sie unterFinden Sie die erforderlichen Kennungen.
- Diese Richtlinienerklärungen ermöglichen es allen Ihren AWS verwalteten Anwendungen und allen IAM-Prinzipalen (Anwendungsadministratoren) in der AWS Organisation, kms: Decrypt mithilfe von IAM Identity Center und Identity Store zu verwenden. Informationen zur Beschränkung dieser Richtlinienerklärungen auf bestimmte AWS verwaltete Anwendungen, Konten oder IAM Identity Center-Instanzen finden Sie unter. Wichtige KMS-Richtlinienerklärungen für Fortgeschrittene

  Sie können den Zugriff auf bestimmte Anwendungsadministratoren einschränken, indem Sie ihn durch bestimmte IAM-Prinzipale * ersetzen. Um sich vor Änderungen der IAM-Rollennamen bei der Neuerstellung von Berechtigungssätzen zu schützen, verwenden Sie den Ansatz in. Beispiel für eine benutzerdefinierte Vertrauensrichtlinie Weitere Informationen finden Sie unter Überlegungen zur Auswahl grundlegender und erweiterter KMS-Richtlinien.

Wichtige KMS-Richtlinienerklärungen

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAppAdminsInTheSameOrganizationToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgID": "o-a1b2c3d4e5"
        },
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "*"
        }
      }
    },
```

```
    {
      "Sid": "AllowAppAdminsInTheSameOrganizationToUseTheKMSKeyViaIdentityStore",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgID": "o-a1b2c3d4e5"
        },
        "StringLike": {
          "kms:ViaService": "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
        }
      }
    },
    {
      "Sid": "AllowManagedAppsToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "*"
        },
        "Bool": {
          "aws:PrincipalIsAWSService": "true"
        },
        "StringEquals": {
          "aws:SourceOrgID": "o-a1b2c3d4e5"
        }
      }
    },
    {
      "Sid": "AllowManagedAppsToUseTheKMSKeyViaIdentityStore",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "identitystore.*.amazonaws.com",
```

```
          "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
        },
        "Bool": {
          "aws:PrincipalIsAWSService": "true"
        },
        "StringEquals": {
          "aws:SourceOrgID": "o-a1b2c3d4e5"
        }
      }
    }
  ]
}
```

Verwenden Sie die folgende Vorlage für IAM-Richtlinienanweisungen[Schritt 4: Konfigurieren Sie IAM-Richtlinien für die kontoübergreifende Verwendung des KMS-Schlüssels](), um Administratoren AWS verwalteter Anwendungen die Verwendung des KMS-Schlüssels von einem Mitgliedskonto aus zu ermöglichen.

- Ersetzen Sie den Beispiel-ARN im Resource-Element durch Ihren tatsächlichen KMS-Schlüssel-ARN. Hilfe bei der Suche nach den Werten der referenzierten Bezeichner finden Sie unter[Finden Sie die erforderlichen Kennungen]().
- Bei einigen AWS verwalteten Anwendungen müssen Sie Berechtigungen für den IAM Identity Center-Dienst konfigurieren. APIs Bevor Sie einen vom Kunden verwalteten Schlüssel in IAM Identity Center konfigurieren, stellen Sie sicher, dass diese Berechtigungen auch die Verwendung des KMS-Schlüssels zulassen. Spezifische Berechtigungsanforderungen für KMS-Schlüssel finden Sie in der Dokumentation der einzelnen AWS verwalteten Anwendungen, die Sie bereitgestellt haben.

Für Administratoren AWS verwalteter Anwendungen sind IAM-Richtlinienerklärungen erforderlich:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid":
 "AllowIAMIdentityCenterAdminToUseTheKMSKeyViaIdentityCenterAndIdentityStore",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "Condition": {
```

```
      "StringLike": {
        "kms:ViaService": [
          "sso.*.amazonaws.com",
          "identitystore.*.amazonaws.com"
        ]
      }
    }
  }]
}
```

Grundlegende KMS-Schlüsselaussage für die Verwendung von AWS Control Tower

Verwenden Sie die folgenden Vorlagen für KMS-SchlüsselanweisungenSchritt 2: Bereiten Sie die wichtigsten Richtlinienerklärungen für KMS vor, um AWS Control Tower Tower-Administratoren die Verwendung des KMS-Schlüssels zu ermöglichen.

- Geben Sie im Principal-Element die IAM-Prinzipale an, die für den Zugriff auf den IAM Identity Center-Dienst verwendet werden. APIs Weitere Informationen zu IAM-Prinzipalen finden Sie im IAM-Benutzerhandbuch unter Einen Prinzipal angeben.
- Diese Richtlinienerklärungen ermöglichen es AWS Control Tower Tower-Administratoren, den KMS-Schlüssel über jede Ihrer IAM Identity Center-Instanzen zu verwenden. AWS Control Tower schränkt jedoch den Zugriff auf die Organisationsinstanz von IAM Identity Center in derselben AWS Organisation ein. Aufgrund dieser Einschränkung hat eine weitere Beschränkung des KMS-Schlüssels auf eine bestimmte IAM Identity Center-Instanz keinen praktischen Nutzen, wie unter beschrieben. Wichtige KMS-Richtlinienerklärungen für Fortgeschrittene
- Um sich vor Änderungen des IAM-Rollennamens bei der Neuerstellung von Berechtigungssätzen zu schützen, verwenden Sie den in der beschriebenen Ansatz. Beispiel für eine benutzerdefinierte Vertrauensrichtlinie

KMS-Schlüsselrichtlinie:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowControlTowerAdminRoleToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/AWSControlTowerExecution"
```

```
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws:sso:instance-arn": "*",
          "kms:ViaService": "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowControlTowerAdminRoleToUseTheKMSKeyViaIdentityStore",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/AWSControlTowerExecution"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
        }
      }
    }
  ]
}
```

AWS Control Tower unterstützt keine delegierte Administration, weshalb Sie keine IAM-Richtlinie für seine Administratoren konfigurieren müssen.

Grundlegende KMS-Schlüssel- und IAM-Richtlinienerklärungen für die Verwendung von IAM Identity Center für Amazon Elastic Compute Cloud Windows-Instances

Verwenden Sie die folgende Vorlage für KMS-Schlüsselrichtlinien, Schritt 2: Bereiten Sie die wichtigsten Richtlinienerklärungen für KMS vor um Benutzern von Single Sign-On (SSO) bei Amazon EC2 Windows-Instances die kontenübergreifende Verwendung des KMS-Schlüssels zu ermöglichen.

- Geben Sie im Feld Principal die IAM-Prinzipale an, die für den Zugriff auf das IAM Identity Center verwendet werden. Weitere Informationen zu IAM-Prinzipalen finden Sie im IAM-Benutzerhandbuch unter Einen Prinzipal angeben.

- Diese Richtlinienerklärung ermöglicht es allen Ihren IAM Identity Center-Instances, den KMS-Schlüssel zu verwenden. Informationen zum Einschränken des Zugriffs auf eine bestimmte IAM Identity Center-Instanz finden Sie unter. Wichtige KMS-Richtlinienerklärungen für Fortgeschrittene
- Um sich vor Änderungen der IAM-Rollennamen bei der Neuerstellung von Berechtigungssätzen zu schützen, verwenden Sie den im Beispiel für eine benutzerdefinierte Vertrauensrichtlinie beschriebenen Ansatz.

Grundlegende Erklärung zur KMS-Richtlinie

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowIAMIdentityCenterPermissionSetRoleToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-
east-1/AWSReservedSSO_MyPermissionSet_1a2b3c4d5e6f7g8h"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws:sso:instance-arn": "*",
          "kms:ViaService": "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowIAMIdentityCenterPermissionSetRoleToUseTheKMSKeyViaIdentityStore",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-
east-1/AWSReservedSSO_MyPermissionSet_1a2b3c4d5e6f7g8h"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
        }
```

```
      }
    }
  ]
}
```

Verwenden Sie die folgende Vorlage für IAM-Richtlinienanweisungen[Schritt 4: Konfigurieren Sie IAM-Richtlinien für die kontoübergreifende Verwendung des KMS-Schlüssels](), um SSO für EC2 Windows-Instanzen die Verwendung des KMS-Schlüssels zu ermöglichen.

Hängen Sie die IAM-Richtlinienerklärung an den vorhandenen Berechtigungssatz in IAM Identity Center an, den Sie verwenden, um SSO-Zugriff auf Amazon EC2 Windows-Instances zu gewähren. Beispiele für IAM-Richtlinien finden Sie unter Remote Desktop Protocol-Verbindungen im AWS Systems Manager Manager-Benutzerhandbuch.

- Ersetzen Sie den Beispiel-ARN im Resource-Element durch Ihren tatsächlichen KMS-Schlüssel-ARN. Hilfe bei der Suche nach den Werten der referenzierten Bezeichner finden Sie unter[Finden Sie die erforderlichen Kennungen]().

IAM-Richtlinie für den Berechtigungssatz:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "IAMPolicyToAllowKMSKeyUseViaIdentityCenterAndIdentityStore",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "Condition": {
      "StringLike": {
        "kms:ViaService": [
          "sso.*.amazonaws.com",
          "identitystore.*.amazonaws.com"
        ]
      }
    }
  }]
}
```

Grundlegende KMS-Schlüssel- und IAM-Richtlinienerklärungen für die Verwendung benutzerdefinierter Workflows mit IAM Identity Center

Verwenden Sie die folgenden Vorlagen für wichtige KMS-Richtlinienerklärungen, Schritt 2: Bereiten Sie die wichtigsten Richtlinienerklärungen für KMS vor um benutzerdefinierten Workflows, wie z. B. vom Kunden verwalteten Anwendungen, im AWS Organizations Verwaltungskonto oder im delegierten Administratorkonto die Verwendung des KMS-Schlüssels zu ermöglichen.

- Geben Sie im Principal-Element die IAM-Prinzipale an, die für den Zugriff auf den IAM Identity Center-Dienst verwendet werden. APIs Weitere Informationen zu IAM-Prinzipalen finden Sie unter Einen Prinzipal angeben im IAM-Benutzerhandbuch.
- Diese Richtlinienerklärungen ermöglichen es Ihrem Workflow, den KMS-Schlüssel über jede Ihrer IAM Identity Center-Instanzen zu verwenden. Informationen zum Einschränken des Zugriffs auf eine bestimmte IAM Identity Center-Instanz finden Sie unter. Wichtige KMS-Richtlinienerklärungen für Fortgeschrittene
- Um sich vor Änderungen des IAM-Rollennamens bei der Neuerstellung von Berechtigungssätzen zu schützen, verwenden Sie den in der beschriebenen Ansatz. Beispiel für eine benutzerdefinierte Vertrauensrichtlinie

KMS-Schlüsselrichtlinie:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCustomWorkflowToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyCustomWorkflowRole"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws:sso:instance-arn": "*",
          "kms:ViaService": "sso.*.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid": "AllowCustomWorkflowToUseTheKMSKeyViaIdentityStore",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyCustomWorkflowRole"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
        }
      }
    }
  ]
}
```

Verwenden Sie die folgende Vorlage für IAM-Richtlinienanweisungen, Schritt 4: Konfigurieren Sie IAM-Richtlinien für die kontoübergreifende Verwendung des KMS-Schlüssels um dem mit dem benutzerdefinierten Workflow verknüpften IAM-Prinzipal die kontenübergreifende Verwendung des KMS-Schlüssels zu ermöglichen. Fügen Sie die IAM-Richtlinienerklärung zum IAM-Prinzipal hinzu.

- Ersetzen Sie den Beispiel-ARN im Resource-Element durch Ihren tatsächlichen KMS-Schlüssel-ARN. Hilfe bei der Suche nach den Werten der referenzierten Bezeichner finden Sie unterFinden Sie die erforderlichen Kennungen.

IAM-Richtlinienerklärung (nur für die kontoübergreifende Verwendung erforderlich):

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowCustomWorkflowToUseTheKMSKeyViaIdentityCenterAndIdentityStore",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "Condition": {
      "StringLike": {
        "kms:ViaService": [
          "sso.*.amazonaws.com",
          "identitystore.*.amazonaws.com"
```

```
        ]
      }
    }
  }]
}
```

Wichtige KMS-Richtlinienerklärungen für Fortgeschrittene

Verwenden Sie erweiterte Richtlinienerklärungen für KMS-Schlüssel, um detailliertere Zugriffskontrollen für Ihren vom Kunden verwalteten KMS-Schlüssel zu implementieren. Diese Richtlinien bauen auf dem auf, Grundlegende KMS-Schlüssel- und IAM-Richtlinienerklärungen indem sie Verschlüsselungskontextbedingungen und dienstspezifische Einschränkungen hinzufügen. Bevor Sie entscheiden, ob Sie erweiterte KMS-Schlüsselrichtlinienerklärungen verwenden möchten, sollten Sie sich mit den entsprechenden Überlegungen vertraut machen.

Verwenden Sie den Verschlüsselungskontext, um den Zugriff einzuschränken

Sie können die Verwendung von KMS-Schlüsseln auf eine bestimmte IAM Identity Center-Instanz beschränken, indem Sie in Ihren wichtigsten Richtlinienerklärungen eine Bedingung für den Verschlüsselungskontext angeben. In den grundlegenden wichtigen Richtlinienaussagen ist dieser Kontext bereits mit einem generischen Wert enthalten. Ersetzen Sie den Platzhalter „*“ durch einen bestimmten Identity Center-Instanz-ARN und einen Identity Store-ARN, um sicherzustellen, dass der Schlüssel nur mit Ihrer beabsichtigten Instanz funktioniert. Sie können der IAM-Richtlinie, die für die kontoübergreifende Verwendung des KMS-Schlüssels konfiguriert ist, auch dieselben Bedingungen für den Verschlüsselungskontext hinzufügen.

Identity Center

```
"StringEquals": {
    "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/
ssoins-1234567890abcdef"
}
```

Identity Store

```
"StringEquals": {
    "kms:EncryptionContext:aws:identitystore:identitystore-arn":
 "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
```

```
}
```

Wenn Sie Hilfe bei der Suche nach diesen Identifikatoren benötigen, finden Sie weitere Informationen unter. Finden Sie die erforderlichen Kennungen

> **Note**
>
> Sie können einen vom Kunden verwalteten KMS-Schlüssel nur mit einer Organisationsinstanz von IAM Identity Center verwenden. Der vom Kunden verwaltete Schlüssel muss sich im Verwaltungskonto der AWS Organisation befinden. Dadurch wird sichergestellt, dass der Schlüssel mit einer einzelnen IAM Identity Center-Instanz verwendet wird. Der Verschlüsselungskontextmechanismus bietet jedoch einen unabhängigen technischen Schutz für die Verwendung einer einzelnen Instanz. Sie können den `aws:SourceArn` Bedingungsschlüssel auch in den KMS-Schlüsselrichtlinienerklärungen verwenden, die für die Identity Center- und Identity Store-Dienstprinzipale vorgesehen sind.

Überlegungen zur Implementierung von Verschlüsselungskontextbedingungen

Bevor Sie die Bedingungen für den Verschlüsselungskontext implementieren, sollten Sie die folgenden Anforderungen überprüfen:

- DescribeKey Aktion. Der Verschlüsselungskontext kann nicht auf die Aktion „kms:DescribeKey“ angewendet werden, die von IAM Identity Center-Administratoren verwendet werden kann. Schließen Sie bei der Konfiguration Ihrer KMS-Schlüsselrichtlinie den Verschlüsselungskontext für diese spezielle Aktion aus, um den ordnungsgemäßen Betrieb Ihrer IAM Identity Center-Instanz sicherzustellen.
- Einrichtung einer neuen Instanz. Wenn Sie eine neue IAM Identity Center-Instanz mit einem vom Kunden verwalteten KMS-Schlüssel aktivieren, finden Sie weitere Informationen unterÜberlegungen zu vom Kunden verwalteten KMS-Schlüsseln und erweiterten KMS-Schlüsselrichtlinien.
- Änderungen der Identitätsquelle. Wenn Sie Ihre Identitätsquelle zu oder von Active Directory ändern, muss dem Verschlüsselungskontext besondere Aufmerksamkeit geschenkt werden. Siehe Überlegungen zur Änderung Ihrer Identitätsquelle.

Richtlinienvorlagen

Wählen Sie je nach Ihren Sicherheitsanforderungen aus diesen erweiterten Richtlinienvorlagen. Sorgen Sie für ein ausgewogenes Verhältnis zwischen detaillierten Zugriffskontrollen und dem damit verbundenen Verwaltungsaufwand.

Themen, die hier behandelt werden:

- KMS-Richtlinienanweisungen für die schreibgeschützte Verwendung einer bestimmten IAM Identity Center-Instanz. In diesem Abschnitt wird die Verwendung des Verschlüsselungskontextes für den schreibgeschützten Zugriff auf IAM Identity Center demonstriert.
- Die wichtigsten KMS-Richtlinienerklärungen für die Verwendung verwalteter Anwendungen wurden verfeinert AWS. In diesem Abschnitt wird gezeigt, wie Sie die KMS-Schlüsselrichtlinien für AWS verwaltete Anwendungen mithilfe des Verschlüsselungskontextes und der Anwendungsinformationen wie dem Anwendungsdienstprinzipal, dem Anwendungs-ARN und der AWS Konto-ID verfeinern können.

KMS-Richtlinienanweisungen für die schreibgeschützte Verwendung einer bestimmten IAM Identity Center-Instanz

Diese Richtlinie ermöglicht es Sicherheitsprüfern und anderen Mitarbeitern, die nur Lesezugriff auf IAM Identity Center benötigen, den KMS-Schlüssel zu verwenden.

So verwenden Sie diese Richtlinie:

1. Ersetzen Sie das Beispiel für schreibgeschützte Administrator-IAM-Prinzipale durch Ihre tatsächlichen Administrator-IAM-Prinzipale
2. Ersetzen Sie den Beispiel-ARN für eine IAM Identity Center-Instanz durch Ihren tatsächlichen Instanz-ARN
3. Ersetzen Sie den Beispiel-Identity Store-ARN durch Ihren tatsächlichen Identity Store-ARN
4. Wenn Sie delegierte Administration verwenden, finden Sie weitere Informationen unter Schritt 4: Konfigurieren Sie IAM-Richtlinien für die kontoübergreifende Verwendung des KMS-Schlüssels

Wenn Sie Hilfe bei der Suche nach den Werten dieser Bezeichner benötigen, finden Sie unter. Finden Sie die erforderlichen Kennungen

Nachdem Sie die Vorlage mit Ihren Werten aktualisiert haben, kehren Sie zu zurück, Schritt 2: Bereiten Sie die wichtigsten Richtlinienerklärungen für KMS vor um bei Bedarf weitere wichtige KMS-Richtlinienerklärungen vorzubereiten.

Die Aktion kms: Entschlüsseln allein schränkt den Zugriff nicht auf schreibgeschützte Operationen ein. Die IAM-Richtlinie muss den schreibgeschützten Zugriff auf den IAM Identity Center-Dienst erzwingen. APIs

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowReadOnlyAccessToIdentityCenterAPI",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyAdminRole"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/
ssoins-1234567890abcdef",
          "kms:ViaService": "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowReadOnlyAccessToIdentityStoreAPI",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyAdminRole"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn":
 "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
        }
      }
    }
```

```
  ]
}
```

Die wichtigsten KMS-Richtlinienerklärungen für die Verwendung verwalteter Anwendungen wurden verfeinert AWS

Diese Richtlinienvorlagen bieten eine detailliertere Kontrolle darüber, welche AWS verwalteten Anwendungen Ihren KMS-Schlüssel verwenden können.

> **Note**
>
> Einige AWS verwaltete Anwendungen können nicht mit IAM Identity Center verwendet werden, das mit einem vom Kunden verwalteten KMS-Schlüssel konfiguriert ist. Sehen Sie sich AWS verwaltete Anwendungen an, die Sie mit IAM Identity Center verwenden können.

Grundlegende KMS-Schlüssel- und IAM-Richtlinienerklärungen für die Verwendung verwalteter Anwendungen AWSSie ermöglichen es jeder AWS verwalteten Anwendung von jedem Konto in derselben AWS Organisation, den KMS-Schlüssel zu verwenden. Verwenden Sie diese verfeinerten Richtlinien, um den Zugriff wie folgt einzuschränken:

- Principal des Anwendungsdienstes
- Anwendungsinstanz ARNs
- AWS Konto IDs
- Verschlüsselungskontext für bestimmte IAM Identity Center-Instanzen

> **Note**
>
> Ein Service Principal ist eine eindeutige Kennung für einen AWS Service, die normalerweise als servicename.amazonaws.com formatiert ist (z. B. elasticmapreduce.amazonaws.com für Amazon EMR).

Nach Konto einschränken

Diese Vorlage für eine KMS-Schlüsselrichtlinie ermöglicht es einer AWS verwalteten Anwendung in bestimmten AWS Konten, den KMS-Schlüssel mithilfe einer bestimmten IAM Identity Center-Instanz zu verwenden.

So verwenden Sie diese Richtlinie:

1. Ersetzen Sie den Beispiel-Serviceprinzipal durch Ihren tatsächlichen Anwendungsdienstprinzipal
2. Ersetzen Sie das Beispielkonto IDs durch das tatsächliche Konto IDs , auf dem Ihre AWS verwalteten Anwendungen bereitgestellt werden
3. Ersetzen Sie den Beispiel-Identity Store-ARN durch Ihren tatsächlichen Identity Store-ARN
4. Ersetzen Sie den Beispiel-ARN für eine IAM Identity Center-Instanz durch Ihren tatsächlichen Instanz-ARN

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowServiceInSpecificAccountsToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "Service": "myapp.amazonaws.com"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": [
            "111122223333",
            "444455556666"
          ]
        },
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/
ssoins-1234567890abcdef"
        },
        "Bool": {
          "aws:PrincipalIsAWSService": "true"
        }
      }
    },
    {
      "Sid": "AllowServiceInSpecificAccountsToUseTheKMSKeyViaIdentityStore",
      "Effect": "Allow",
      "Principal": {
```

```
        "Service": "myapp.amazonaws.com"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": [
            "111122223333",
            "444455556666"
          ]
        },
        "StringLike": {
          "kms:ViaService": "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn":
 "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
        },
        "Bool": {
          "aws:PrincipalIsAWSService": "true"
        }
      }
    }
  ]
}
```

Nach Anwendungsinstanz einschränken

Diese Vorlage für eine KMS-Schlüsselrichtlinie ermöglicht es einer bestimmten AWS verwalteten Anwendungsinstanz, den KMS-Schlüssel mithilfe einer bestimmten IAM Identity Center-Instanz zu verwenden.

So verwenden Sie diese Richtlinie:

1. Ersetzen Sie den Beispiel-Serviceprinzipal durch Ihren tatsächlichen Anwendungsdienstprinzipal
2. Ersetzen Sie den ARN der Beispielanwendung durch den ARN Ihrer tatsächlichen Anwendungsinstanz
3. Ersetzen Sie den Beispiel-Identity Store-ARN durch Ihren tatsächlichen Identity Store-ARN
4. Ersetzen Sie den Beispiel-ARN für eine IAM Identity Center-Instanz durch Ihren tatsächlichen Instanz-ARN

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

```
  "Statement": [
    {
      "Sid": "AllowSpecificAppInstanceToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "Service": "myapp.amazonaws.com"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceARN": "arn:aws:myapp:us-east-1:111122223333:application/my-
application"
        },
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/
ssoins-1234567890abcdef"
        },
        "Bool": {
          "aws:PrincipalIsAWSService": "true"
        }
      }
    },
    {
      "Sid": "AllowSpecificAppInstanceToUseTheKMSKeyViaIdentityStore",
      "Effect": "Allow",
      "Principal": {
        "Service": "myapp.amazonaws.com"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceARN": "arn:aws:myapp:us-east-1:111122223333:application/my-
application"
        },
        "StringLike": {
          "kms:ViaService": "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn":
 "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
        },
        "Bool": {
          "aws:PrincipalIsAWSService": "true"
```

```
        }
      }
    }
  ]
}
```

Überlegungen zu vom Kunden verwalteten KMS-Schlüsseln und erweiterten KMS-Schlüsselrichtlinien

Bei der Implementierung von vom Kunden verwalteten KMS-Schlüsseln mit IAM Identity Center sollten Sie diese Faktoren berücksichtigen, die sich auf die Einrichtung, Sicherheit und laufende Wartung Ihrer Verschlüsselungskonfiguration auswirken.

Überlegungen zur Auswahl grundlegender und erweiterter KMS-Richtlinien

Bei der Entscheidung, ob die Verwendung der KMS-Schlüsselberechtigungen spezifischer gestaltet werden sollWichtige KMS-Richtlinienerklärungen für Fortgeschrittene, sollten Sie den Verwaltungsaufwand und die Sicherheitsanforderungen Ihres Unternehmens berücksichtigen. Spezifischere Richtlinienerklärungen bieten eine genauere Kontrolle darüber, wer den Schlüssel verwenden kann und für welche Zwecke. Sie müssen jedoch fortlaufend gewartet werden, wenn sich Ihre IAM Identity Center-Konfiguration weiterentwickelt. Wenn Sie beispielsweise die Verwendung des KMS-Schlüssels auf bestimmte AWS verwaltete Anwendungsbereitstellungen beschränken, müssen Sie die Schlüsselrichtlinie jedes Mal aktualisieren, wenn Ihre Organisation eine Anwendung bereitstellen oder deren Bereitstellung aufheben möchte. Weniger restriktive Richtlinien reduzieren den Verwaltungsaufwand, gewähren jedoch möglicherweise umfassendere Berechtigungen, als für Ihre Sicherheitsanforderungen erforderlich sind.

Überlegungen zur Aktivierung einer neuen IAM Identity Center-Instanz mit einem vom Kunden verwalteten KMS-Schlüssel

Die hier aufgeführten Überlegungen gelten, wenn Sie den Verschlüsselungskontext verwenden, wie unter Beschränken der Verwendung des KMS-Schlüssels auf eine bestimmte IAM Identity Center-Instanz beschrieben. Wichtige KMS-Richtlinienerklärungen für Fortgeschrittene

Wenn Sie eine neue IAM Identity Center-Instanz mit einem vom Kunden verwalteten KMS-Schlüssel aktivieren, ARNs sind das IAM Identity Center und der Identity Store erst nach der Einrichtung verfügbar. Ihnen stehen folgende Optionen zur Verfügung:

- Verwenden Sie vorübergehend generische ARN-Muster und ersetzen Sie sie dann durch full, ARNs nachdem die Instanz aktiviert wurde. Denken Sie daran, nach Bedarf zwischen den StringLike Operatoren StringEquals und zu wechseln.
  - Für IAM Identity Center SPN: „arn: $ {Partition} :sso: ::instance/*“.
  - Für Identity Store SPN: „arn: $ {Partition} :identitystore: :$ {Account} :identitystore/*“.
- Verwenden Sie vorübergehend „purpose:KEY_CONFIGURATION“ im ARN. Dies funktioniert nur bei der Instanzaktivierung und muss durch den tatsächlichen ARN ersetzt werden, damit Ihre IAM Identity Center-Instanz normal funktioniert. Der Vorteil dieses Ansatzes besteht darin, dass Sie nicht vergessen können, diesen zu ersetzen, nachdem die Instanz aktiviert wurde.
  - Verwenden Sie für IAM Identity Center SPN: „arn: $ {Partition} :sso: ::instance/purpose:KEY_CONFIGURATION“
  - Verwenden Sie für Identity Store SPN: „arn: $ {Partition} :identitystore: :$ {Account} :identityStore/purpose:KEY_CONFIGURATION“

  > **Important**
  >
  > Wenden Sie diese Konfiguration nicht auf einen KMS-Schlüssel an, der bereits in einer vorhandenen IAM Identity Center-Instanz verwendet wird, da dies den normalen Betrieb stören kann.

- Lassen Sie die Bedingung für den Verschlüsselungskontext in der KMS-Schlüsselrichtlinie weg, bis die Instanz aktiviert ist.

Ressourcen taggen AWS IAM Identity Center

Ein Tag ist eine benutzerdefinierte Attributbezeichnung, die Sie einer AWS Ressource hinzufügen, um die Identifizierung, Organisation und Suche nach Ressourcen zu erleichtern. 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 auf eine leere Zeichenfolge festlegen, aber Sie können den Wert eines Tags nicht auf Null setzen. Ein nicht angegebener Tag-Wert entspricht einer leeren Zeichenfolge.

Mithilfe von Tags können Sie Ihre AWS Ressourcen identifizieren und organisieren. Viele AWS Dienste unterstützen Tagging, sodass Sie Ressourcen aus verschiedenen Diensten dasselbe Tag zuweisen können, um anzuzeigen, dass die Ressourcen miteinander verknüpft sind. Sie können beispielsweise dasselbe Tag einem bestimmten Berechtigungssatz in Ihrer Instanz von IAM Identity Center zuweisen. Weitere Informationen zu Tagging-Strategien finden Sie unter Tagging AWS Resources im Allgemeine AWS-Referenz Guide 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.

Sie können 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 das IAM Identity Center verwenden, APIs 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.

Themen

Tag-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.
- Nicht `aws:` als Präfix für Schlüssel verwenden; es ist für die Verwendung reserviert AWS

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.
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 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.

AWS CLI Beispiele

Das AWS CLI stellt Befehle bereit, 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
```

Verwalten Sie Tags mithilfe der IAM Identity Center-API

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 von AWS CLI mit IAM Identity Center

AWS Die Integration von Command Line Interface (CLI) Version 2 mit IAM Identity Center vereinfacht den Anmeldevorgang. Entwickler können sich direkt AWS CLI mit den gleichen Active Directory- oder IAM Identity Center-Anmeldeinformationen anmelden, die sie normalerweise für die Anmeldung bei IAM Identity Center verwenden, und auf die ihnen zugewiesenen Konten und Rollen zugreifen. Wenn ein Administrator beispielsweise IAM Identity Center für die Verwendung von Active Directory für die Authentifizierung konfiguriert hat, kann sich ein Entwickler AWS CLI direkt mit seinen Active Directory-Anmeldeinformationen anmelden.

AWS Die CLI-Integration mit IAM Identity Center bietet die folgenden Vorteile:

- Unternehmen können es ihren Entwicklern ermöglichen, sich mit Anmeldeinformationen von IAM Identity Center oder Active Directory anzumelden, indem sie IAM Identity Center über ihr Active Directory verbinden. Directory Service
- Entwickler können sich für einen schnelleren Zugriff über die CLI anmelden.
- Entwickler können Konten und Rollen, denen sie Zugriff zugewiesen haben, auflisten und zwischen ihnen wechseln.
- Entwickler können automatisch benannte Rollenprofile in ihrer CLI-Konfiguration 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 beginnen und dort bleiben und Skripts mit langer Laufzeit ausführen können.

So integrieren Sie AWS CLI in IAM Identity Center

Um die AWS CLI-Integration mit IAM Identity Center zu verwenden, laden Sie AWS Command Line Interface Version 2 herunter, installieren und konfigurieren Sie sie. Ausführliche Schritte zum Herunterladen und zur Integration AWS CLI mit IAM Identity Center finden Sie unter Konfiguration der AWS CLI für die Verwendung von IAM Identity Center im AWS Command Line Interface Benutzerhandbuch.

Überlegungen zum AWS-Managementkonsole privaten Zugriff

Wenn Ihr Unternehmen die AWS-Managementkonsole Private Access-Funktion verwendet, sollten Sie sich überlegen, wie sich Ihre Benutzer bei IAM Identity Center anmelden.

Eine VPC-Endpunktrichtlinie schränkt die Anmeldung an der Verwaltungskonsole ein, wodurch verhindert wird, dass sich Ihre Benutzer dort anmelden, zu deren Zugriff AWS-Konten sie nicht berechtigt sind. Weitere Informationen finden Sie unter AWS-Managementkonsole Private Access im Handbuch AWS-Managementkonsole Erste Schritte.

VPC-Endpunkte blockieren die Anmeldung beim IAM Identity Center

Es ist wichtig zu beachten, dass die Verwendung von VPC-Endpunkten die Anmeldung beim IAM Identity Center blockiert. Dies passiert, wenn ein Benutzer bereits über den VPC-Endpunkt bei der Managementkonsole angemeldet ist. Um sicherzustellen, dass sich Ihre Benutzer weiterhin bei IAM Identity Center anmelden können, müssen sie den öffentlichen Endpunkt für die AWS Anmeldung verwenden und nicht den VPC-Endpunkt.

Kontingente und Limits in IAM Identity Center

In den folgenden Tabellen werden die Kontingente in IAM Identity Center beschrieben. Anfragen zur Erhöhung des Kontingents müssen von einem Verwaltungskonto oder einem delegierten Administratorkonto stammen. Informationen zur Erhöhung eines Kontingents finden Sie unter Eine Kontingenterhöhung beantragen.

> **Note**
>
> Wir empfehlen die Verwendung der AWS CLI und APIs die Verwaltung von IAM Identity Center, wenn Sie mehr als 50.000 Benutzer, 10.000 Gruppen oder 500 Berechtigungssätze haben. Weitere Informationen zur CLI finden Sie unterIntegration von AWS CLI mit IAM Identity Center. Weitere Informationen zu APIs finden Sie unter Willkommen bei der IAM Identity Center API-Referenz.

Kontingente für Anwendungen

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 das IAM Identity Center hochgeladenen IdP-Zertifikats	2500 (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	3500	Ja
Anzahl der bereitgestellten Berechtigungssätze, die pro Person zulässig sind AWS-Konto	500	Ja
Anzahl der eingebundenen Richtlinien pro Berechtigungssatz	1	Nein
Anzahl der AWS 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 in der Service Quota-Konsole für jeden,

für den Sie den Berechtigungssatz bereitstellen möchten, eine Erhöhung des IAM-Kontingents an verwaltete Richtlinien AWS-Konto an, die einer IAM-Rolle zugeordnet sind.

> **Note**
>
> AWS-Konten Mit Berechtigungssätzen verwaltenwerden AWS-Konten als IAM-Rollen bereitgestellt oder verwenden bestehende IAM-Rollen in und halten sich daher an AWS-Konten IAM-Kontingente. Weitere Informationen zu Kontingenten, die mit IAM-Rollen verknüpft sind, finden Sie unter IAM- und STS-Kontingente.

Active Directory-Kontingente

Ressource	Standardkontingent	Kann erhöht werden
Anzahl der gleichzeitig möglichen verbundenen Verzeichnisse	1	Nein

Kontingente für den Identitätsspeicher von IAM Identity Center

Ressource	Standardkontingent	Kann erhöht werden
Anzahl unterstützter Benutzer in IAM Identity Center	100000	Ja
Anzahl unterstützter Gruppen in IAM Identity Center	100000	Ja
Anzahl der eindeutigen Gruppen, die zum Auswerten der Berechtigungen für einen Benutzer verwendet werden können	1000	Nein

Grenzwerte für die Drosselung von IAM Identity Center

Ressource	Standardkontingent
IAM Identity Center APIs	Für IAM Identity Center APIs gilt ein kollektives Drossellimit von 20 Transaktionen pro Sekunde (TPS). Sie können einen Support-Fall eröffnen, um eine Erhöhung des Limits zu beantragen. Die CreateAccountAssignmentAPI hat ein Limit von 15 ausstehenden asynchronen Aufrufen. Dieses Limit kann nicht erhöht werden.
Identitätsspeicher APIs	Identity Store APIs hat ein Drossellimit von 20 Transaktionen pro Sekunde (TPS) pro API. Dieses Limit gilt pro Identity Store-Instanz. Sie können einen Support-Fall eröffnen, um eine Erhöhung des Limits zu beantragen.
SCIM APIs	SCIM APIs hat Drosselgrenzen von 25 Transaktionen pro Sekunde (TPS) für Schreibvorgänge APIs und 40 TPS für Lesevorgänge. APIs Diese Grenzwerte gelten pro Identity Store-Instanz. Sie können einen Support-Fall eröffnen, um eine Erhöhung des Limits zu beantragen.

Kontingente für OIDC-Serviceanfragen

Ressource	Standardwert (Anforderungen pro Sekunde)	Kann erhöht werden
Anforderungsrate von einer Remote-Adresse zur Registrierung eines öffentlichen Clients OAuth	20	Ja

Ressource	Standardwert (Anforderungen pro Sekunde)	Kann erhöht werden
Gilt für: RegisterClient		
Anfragerate von einem öffentlichen Kunden, der beim OIDC-Service registriert ist Gilt für:, CreateToken StartDeviceAuthorization	80	Ja
Anforderungsrate von allen öffentlichen Clients, die bei derselben IAM Identity Center-Instanz registriert sind Gilt für: CreateToken	250	Ja
Anforderungsrate von einer IAM Identity Center-An wendung, die bei der IAM Identity Center-Instanz registriert ist Gilt für: IAM CreateTokenWith	80	Ja
Token-Generierungsrate für alle IAM Identity Center-An wendungen, die bei derselben IAM Identity Center-Instance registriert sind, mit JWT Bearer Grant Gilt für: IAM CreateTokenWith	10	AWS Support kontaktieren

Zusätzliche Kontingente

Ressource	Standardkontingent	Kann erhöht werden
Gesamtzahl der AWS-Konten Anwendungen, die konfiguriert werden können * **	3000	Ja
Gesamtzahl der IAM Identity Center-Instanzen pro Konto	1	Nein
Gesamtzahl der vertrauen swürdigen Token-Emittenten	10	Nein

* Sie könnten beispielsweise 2750 Konten und 250 Anwendungen konfigurieren, was insgesamt 3000 Konten und Anwendungen ergibt.

** Der `ProvisionPermissionSet`API-Vorgang kann einen Berechtigungssatz mit der Option `ALL_PROVISIONED_ACCOUNTS` bis maximal 3500 AWS-Konten bereitstellen. Wenn Sie einen Berechtigungssatz für mehr als 3500 bereitstellen müssen AWS-Konten, können Sie den `ProvisionPermissionSet` API-Vorgang mit der `AWS_ACCOUNT` Option verwenden, die den Berechtigungssatz in einem einzigen bereitstellt AWS-Konto. Sie können bis zu drei gleichzeitige Aufrufe von tätigen. `ProvisionPermissionSet`

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 zulässt, `sso:ListApplications` aber nicht. APIs 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": "sso:ListApplicationProviders",
         "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": "sso: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": "sso:ListApplicationProviders",
         "Resource": "*"
    }
]
```

Wenn Ihre Richtlinien aktualisiert werden, wenden Sie sich an uns, 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 Ihr Identity Provider (IdP) so konfiguriert ist, dass er Benutzer mithilfe der SCIM-Synchronisierung für das IAM Identity Center bereitstellt, kann es bei der Benutzerbereitstellung zu Synchronisierungsfehlern kommen. Dies kann darauf hindeuten, dass die Benutzerkonfiguration in Ihrem IdP nicht mit den IAM Identity Center-Anforderungen kompatibel ist. In diesem Fall gibt das IAM Identity Center SCIM Fehlermeldungen zurück, APIs die Aufschluss über die Ursache des Problems geben. Sie finden diese Fehlermeldungen in den Protokollen oder in der

Benutzeroberfläche Ihres IdP. Alternativ finden Sie in den Protokollen möglicherweise detailliertere Informationen zu den Bereitstellungsfehlern.AWS CloudTrail

Weitere Informationen zu den IAM Identity Center SCIM-Implementierungen, einschließlich der Spezifikationen der erforderlichen, optionalen und nicht unterstützten Parameter und Operationen für Benutzerobjekte, finden Sie im IAM Identity Center SCIM Implementation Developer Guide im SCIM Developer Guide

Im Folgenden sind einige der häufigsten Gründe für diesen Fehler aufgeführt:

1. Dem Benutzerobjekt im IdP fehlt ein Vorname (Vorname), ein Nachname (Familien) und and/or ein Anzeigename.

   Fehlermeldung: „`'name.givenName'` Es wurden 2 Validierungsfehler festgestellt: Wert at hat die Einschränkung nicht erfüllt: Das Mitglied muss den regulären Ausdruck erfüllen; Muster: [\\ p {L}\\ p {M}\\ p {S}\\ p {N}\\ p {P}\\ t\\n\\ r] +; Wert bei `'name.givenName'` konnte die Einschränkung nicht erfüllt werden: Mitglied muss eine Länge größer oder gleich 1 haben.

   - Lösung: Fügen Sie einen ersten (angegebenen), 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.

   Fehlermeldung: „Das Listenattribut `emails` überschreitet den zulässigen Grenzwert von 1“

   - 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.

Beim Bereitstellen von Benutzern oder Gruppen mit einem externen Identitätsanbieter ist ein Fehler beim Duplizieren von Benutzern oder Gruppen aufgetreten

Wenn bei der Bereitstellung von Benutzern oder Gruppen in einem externen Identitätsanbieter (IdP) Probleme mit der IAM Identity Center-Synchronisierung auftreten, kann dies daran liegen, dass Ihre externen IdP-Benutzer oder Gruppen keine eindeutigen Attributwerte haben. Möglicherweise erhalten Sie die folgenden Fehlermeldungen in Ihrem externen IdP:

Hat sich geweigert, eine neue, doppelte Ressource zu erstellen

Dieses Problem kann in den folgenden Szenarien auftreten:

- Szenario 1
  - Sie verwenden benutzerdefinierte, nicht eindeutige Attribute in Ihrem externen IdP für Attribute, die in IAM Identity Center eindeutig sein müssen. Bestehende IAM Identity Center-Benutzer oder -Gruppen können nicht mit Ihrem IdP synchronisiert werden.
- Szenario 2
  - Sie versuchen, Benutzer mit doppelten Attributen für Attribute zu erstellen, die in IAM Identity Center eindeutig sein müssen.

- Sie erstellen beispielsweise einen IAM Identity Center-Benutzer mit den folgenden Attributen oder verfügen bereits über einen solchen:
  - Benutzername: Jane Doe
  - Primäre E-Mail-Adresse: `jane_doe@example.com`
- Dann versuchen Sie, einen anderen Benutzer in Ihrem externen IdP mit den folgenden Attributen zu erstellen:
  - Benutzername: Richard Doe
  - Primäre E-Mail-Adresse: `jane_doe@example.com`
    - Der externe IdP versucht, den Benutzer im IAM Identity Center zu synchronisieren und zu erstellen. Diese Aktionen schlagen jedoch fehl, da beide Benutzer doppelte Werte für eine primäre E-Mail-Adresse haben, die eindeutig sein muss.

Der Benutzername, die primäre E-Mail-Adresse und die externe ID müssen eindeutig sein, damit Ihre externen IdP-Benutzer erfolgreich mit IAM Identity Center synchronisieren können. Ebenso muss der Gruppenname eindeutig sein, damit Ihre externen IdP-Gruppen erfolgreich mit IAM Identity Center synchronisiert werden können.

Die Lösung besteht darin, die Attribute Ihrer Identitätsquelle zu überprüfen und sicherzustellen, dass sie eindeutig sind.

Benutzer können sich nicht anmelden, wenn ihr Benutzername im UPN-Format ist

Benutzer können sich aufgrund des Formats, das sie zur 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 MFA für Identity Center-Verzeichnisbenutzer. 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 'SSO_' beginnen. AWSReserved 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 den Ereignisnamen ExternalIdPDirectoryLogin aufrufen AWS CloudTrail und danach 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 browser/platform zum FIDO2Support unter: Webauthentifizierung (WebAuthn). Weitere Informationen zu WebAuthn in IAM Identity Center finden Sie unterFIDO2 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 gleichwertigen Quellen übereinstimmt. local/regional

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 das IAM Identity Center hochgeladene IdP-Zertifikat mit dem übereinstimmt, das von Ihrem IdP bereitgestellt wurde. Sie können das Zertifikat von der IAM Identity Center-Konsole aus überprüfen, indem Sie zu Einstellungen navigieren. Wählen Sie auf der Registerkarte „Identitätsquelle“ die Option „Aktion“ und anschließend „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 nicht delete/modify/remove/assign auf die im Verwaltungskonto bereitgestellten Berechtigungssätze zugreifen

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 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.

Problembehandlung bei vom Kunden verwalteten Schlüsseln in AWS IAM Identity Center

In diesem Thema werden häufig auftretende Fehler im Zusammenhang mit kundenverwalteten Schlüsseln beschrieben, die bei der Verwendung auftreten können, AWS IAM Identity Center und es werden Schritte zur Behebung dieser Fehler beschrieben.

Zugriff verweigert: Problem mit der KMS Decrypt-Berechtigung

Fehler: „Der Benutzer xxxxxxx ist nicht berechtigt, die mit diesem Chiffretext verknüpfte Ressource zu kms: entschlüsseln, da keine identitätsbasierte Richtlinie die Aktion Entschlüsseln zulässt“ kms:

Dem Benutzer oder IAM-Prinzipal fehlen die erforderlichen `kms:Decrypt` Berechtigungen in seiner IAM-Richtlinie oder KMS-Schlüsselrichtlinie.

Problembehandlung mit: AWS CloudTrail

1. Suchen Sie nach `kms.amazonaws.com` Ereignissen in CloudTrail

2. Suchen Sie nach dem Namen der Veranstaltung `Decrypt`
3. Überprüfen Sie die `errorMessage` Felder `errorCode` und
4. Überprüfen Sie`userIdentity`, welcher Principal den Vorgang versucht hat

Um dieses Problem zu beheben, gewähren Sie dem Benutzer oder dem IAM-Prinzipal `kms:Decrypt` Zugriffsberechtigungen in seiner IAM-Richtlinie und KMS-Schlüsselrichtlinie. Weitere Informationen finden Sie unter Implementierung von vom Kunden verwalteten KMS-Schlüsseln in AWS IAM Identity Center.

AWS Anmeldefehler bei verwalteten Anwendungen, wenn ein vom Kunden verwalteter KMS-Schlüssel im IAM Identity Center aktiviert ist

Wenn sich keine Identity Center-Benutzer bei AWS verwalteten Anwendungen anmelden können und Sie in Ihrer IAM Identity Center-Instanz einen vom Kunden verwalteten KMS-Schlüssel aktiviert haben, stellen Sie sicher, dass die KMS-Schlüsselrichtlinie den AWS verwalteten Anwendungen Berechtigungen zur Verwendung des vom Kunden verwalteten KMS-Schlüssels gewährt. Weitere Informationen finden Sie unter Grundlegende KMS-Schlüssel- und IAM-Richtlinienerklärungen.

AWS Fehler bei der and/or Benutzerzuweisung bei der Installation verwalteter Anwendungen, wenn ein vom Kunden verwalteter KMS-Schlüssel in IAM Identity Center aktiviert ist

Fehler: „Der Benutzer xxxxxxx ist nicht berechtigt, die mit diesem Chiffretext verknüpfte Ressource zu kms: entschlüsseln, da keine identitätsbasierte Richtlinie die Aktion Entschlüsseln zulässt“ kms:

Dem Benutzer oder IAM-Prinzipal fehlen die erforderlichen `kms:Decrypt` Berechtigungen in seiner IAM-Richtlinie oder KMS-Schlüsselrichtlinie.

Problembehandlung mit: CloudTrail

1. Suchen Sie nach dem Namen des Ereignisses `Decrypt`
2. Überprüfen Sie die `errorMessage` Felder `errorCode` und
3. Überprüfen Sie`userIdentity`, welcher Principal den Vorgang versucht hat

Um dieses Problem zu beheben, gewähren Sie dem Benutzer oder dem IAM-Prinzipal `kms:Decrypt` Zugriffsberechtigungen in seiner IAM-Richtlinie und KMS-Schlüsselrichtlinie. Weitere Informationen

finden Sie unter Implementierung von vom Kunden verwalteten KMS-Schlüsseln in AWS IAM Identity Center.

Problem mit den KMS-Berechtigungen: Konfiguration des vom Kunden verwalteten Schlüssels mit AWS IAM Identity Center

Dem Benutzer oder IAM-Prinzipal fehlen eine oder mehrere erforderliche KMS-Berechtigungen (`kms:Decrypt`,,`kms:DescribeKey`) `kms:Encryptkms:GenerateDataKey`, wenn der vom Kunden verwaltete Schlüssel aktiviert wird.

Problembehandlung mit CloudTrail:

1. Suchen Sie nach `DecryptEncrypt`,`GenerateDataKey`, oder `DescribeKey` Ereignissen
2. Überprüfen Sie die `errorMessage` Felder `errorCode` und
3. Überprüfen Sie`userIdentity`, welcher Principal den Vorgang versucht hat

Um dieses Problem zu beheben, gewähren Sie dem Benutzer oder IAM-Prinzipal alle erforderlichen KMS-Berechtigungen in seiner identitätsbasierten Richtlinie oder KMS-Schlüsselrichtlinie. Weitere Informationen finden Sie unter Implementierung von vom Kunden verwalteten KMS-Schlüsseln in AWS IAM Identity Center.

AWS Anmeldefehler beim Zugriffsportal, wenn ein vom Kunden verwalteter KMS-Schlüssel im IAM Identity Center aktiviert ist

Fehler: „FEHLERCODE: 0001 — IdentityCenter Der Dienstzugriff ist blockiert. Wenden Sie sich für weitere Schritte an Ihren IdentityCenter Administrator.“

Wenn sich Benutzer nicht beim AWS Zugriffsportal anmelden können und Sie in Ihrer IAM Identity Center-Instanz einen vom Kunden verwalteten KMS-Schlüssel aktiviert haben, stellen Sie sicher, dass die KMS-Schlüsselrichtlinie Identity Center und Identity Store die erforderlichen Berechtigungen gewährt. Weitere Informationen finden Sie unter Grundlegende KMS-Schlüssel- und IAM-Richtlinienerklärungen.

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: 21. Oktober 2025

Änderung	Beschreibung	Datum
Die AWS verwaltete Richtlinie wurde aktualisiert	Die `AWSIdentityCenterExternalManagementPolicy` AWS verwaltete Richtlinie wurde aktualisiert, um den ARN für die Bereitstellung des Mandanten zu ändern.	5. Dezember 2025
Neues Thema für AWS verwaltete Richtlinien	Es wurden Details für die `AWSIdentityCenterExternalManagementPolicy` AWS verwaltete Richtlinie hinzugefügt.	21. November 2025
Audit und Anleitung zum Abgleich bei der automatischen Bereitstellung	Es wurden Anleitungen zur Prüfung und Abstimmung von automatisch bereitgestellten SCIM-Benutzern, Gruppen und Gruppenmitgliedschaften mithilfe von Identity Store und Befehlen hinzugefügt. APIs AWS CLI	17. Oktober 2025
Kontingente für OIDC-Serviceanfragen	Es wurden Kontingente für OIDC-Serviceanfragen hinzugefügt, einschließlich	13. Oktober 2025

	Ratenbegrenzungen für die OAuth Kundenregistrierung, Token-Erstellung und andere OIDC-Operationen.	
Updates für AWS verwaltete Richtlinien	IAM Identity Center hat die verwalteten RichtlinienAWSSSOMasterAccountAdministrator ,, AWSSSOMemberAccountAdministrator AWSSSOReadOnly AWSSSODirectoryAdministrator , und AWSSSODirectoryReadOnly um die erforderlichen AWS KMS Berechtigungen für IAM Identity Center-Instanzen erweitert, die vom Kunden verwaltete Schlüssel zur Verschlüsselung verwenden.	17. September 2025
Vom Kunden verwaltete Schlüssel für die Verschlüsselung im Ruhezustand	Unterstützung für vom Kunden verwaltete KMS-Schlüssel zur Verschlüsselung von Personaldaten im Ruhezustand wurde hinzugefügt.	17. September 2025
Beispiel für eine ressourcenbasierte Richtlinie, die die Erstellung von Token ermöglicht	Es wurde ein Beispiel für eine ressourcenbasierte Richtlinie hinzugefügt, die die Token-Erstellung für autorisierte Client-Anwendungen ermöglicht.	16. September 2025
Support für Benutzersitzungen im Hintergrund	Inhalt für Benutzersitzungen im Hintergrund hinzugefügt.	11. August 2025

Konsolensitzungen mit verbesserter Identität	Die Terminologie für Konsolensitzungen mit verbesserter Identität (früher bekannt als identitätsbewusste Sitzungen) wurde aktualisiert.	12. Mai 2025
Erste Schritte mit der Reorganisation	Die Inhalte für die ersten Schritte wurden neu organisiert, um die Übersichtlichkeit und das Benutzererlebnis zu verbessern.	6. Mai 2025
IAM Identity Center AD Sync nicht mehr unterstützen	Sie können Active Directory -Benutzer nicht mehr mit IAM Identity Center AD Sync bereitstellen. Stattdessen können Sie das konfigurierbare AD Sync von IAM Identity Center verwenden.	17. April 2025
Der Inhalt für die authentifizierte Sitzung wurde aktualisiert	Aktualisierung der IAM Identity Center-Sitzungsdauer, wenn die Benutzersitzung gelöscht wird.	2. April 2025
Aktualisierungen für verwaltete Richtlinien AWS	Die Berechtigungen für die `AWSSSOServiceRolePolicy` AWS verwaltete Richtlinie wurden aktualisiert.	11. Februar 2025
Der Workflow zur Aktivierung von IAM Identity Center wurde verbessert	Der Workflow für die Aktivierung von Organisationsinstanzen und Kontoinstanzen von IAM Identity Center wurde aktualisiert.	11. Februar 2025

Updates für die Aktivierung von IAM Identity Center	Aktualisierte Inhalte und Verfahren zur Aktivierung von Organisationsinstanzen und Kontoinstanzen von IAM Identity Center.	10. Oktober 2024
Updates für AWS verwaltete Richtlinien	Die Berechtigungen für die `AWSIAMIdentityCenterAllowListForIdentityContext` AWS verwaltete Richtlinie wurden aktualisiert.	2. Oktober 2024
Updates für die AWS verwaltete Richtlinie	Die Berechtigungen für die `AWSSSOMasterAccountAdministrator` AWS verwaltete Richtlinie wurden aktualisiert.	26. September 2024
Updates für die AWS verwaltete Richtlinie	Die Berechtigungen für die `AWSIAMIdentityCenterAllowListForIdentityContext` AWS verwaltete Richtlinie wurden aktualisiert.	4. September 2024
Aktualisierungen zum Thema „Was ist IAM Identity Center?“ Thema	Der Inhalt, der die Vorteile und Funktionen von IAM Identity Center beschreibt, wurde aktualisiert.	19. August 2024
Updates für AWS verwaltete Richtlinien	Die Berechtigungen für die `AWSIAMIdentityCenterAllowListForIdentityContext` AWS verwaltete Richtlinie wurden aktualisiert.	12. Juli 2024

Updates für die AWS verwaltete Richtlinie	Die Berechtigungen für die `AWSIAMIdentityCenterAllowListForIdentityContext` AWS verwaltete Richtlinie wurden aktualisiert.	27. Juni 2024
Updates für die AWS verwaltete Richtlinie	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 die AWS verwaltete Richtlinie	Die Berechtigungen für die `AWSSSOMemberAccountAdministrator` AWS verwaltete Richtlinie wurden aktualisiert.	26. April 2024
Updates für die AWS verwaltete Richtlinie	Die Berechtigungen für die `AWSSSOReadOnly` AWS verwaltete Richtlinie wurden aktualisiert.	26. April 2024

Updates für die AWS verwaltete Richtlinie	Die Berechtigungen für die `AWSIAMIdentityCenterAllowListForIdentityContext` AWS verwaltete Richtlinie wurden aktualisiert.	26. April 2024
Updates für die AWS verwaltete Richtlinie	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 die AWS verwaltete Richtlinie	Die Berechtigungen für die `AWSIAMIdentityCenterAllowListForIdentityContext` AWS verwaltete Richtlinie wurden aktualisiert.	11. April 2024
Updates für die AWS verwaltete Richtlinie	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 das neue Create, Update und Delete 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 Konten und den Zugriff auf Anwendungen für Ihre Belegschaftsbenutzer 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 AWS verwalteter und kundenverwalteter 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	Aktualisierte Berechtigungen für die `AWSSSOMasterAccountAdministrator` `AWSSSOMemberAccountAdministrator` , und `AWSSSOReadOnly` AWS verwalteten Richtlinien.	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 für Okta	Inhalt zur Integration Okta als unterstützter externer Identitätsanbieter hinzugefügt.	28. Mai 2020

Support für externe Identitätsanbieter	Die Verweise vom Verzeichnis 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 hinzugefügt.	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.