ユーザーガイド

AWS IAM Identity Center

AWS IAM Identity Center: ユーザーガイド

Table of Contents

IAM Identity Center とは何ですか?

AWS IAM Identity Center AWS のサービス AWS リソースへのヒューマンユーザーアクセスを管理する場合に推奨されます。workforce identities としても知られるワークフォースユーザーに複数の AWS アカウント およびアプリケーションへの一貫したアクセス許可を 1 か所から割り当てることができます。IAM ID センターは追加料金なしで提供されます。

IAM Identity Center を使用すると、従業員ユーザーを作成または接続し、すべてのユーザーやアプリケーションにわたるアクセスを一元管理できます。 AWS アカウント 「マルチアカウント権限」を使用してワークフォースユーザーに AWS アカウントへのアクセス権を割り当てることができます。アプリケーション割り当てを使用して、 AWS 管理対象アプリケーションと顧客管理型アプリケーションへのアクセス権をユーザーに割り当てることができます。

> **Note**
>
> AWS Single Sign-On というサービス名は廃止されましたが、このガイドでは、ユーザーが 1 回サインインして複数のアプリケーションや Web サイトにアクセスできるようにする認証スキームを説明するために、シングルサインオンという用語が今でも使用されています。

IAM アイデンティティセンター機能

IAM アイデンティティセンターには、次のコア機能と特徴が含まれています。

ワークフォース ID の管理

AWS でワークロードを構築または操作するヒューマンユーザーは、ワークフォースユーザーまたはワークフォース ID とも呼ばれます。ワークフォースユーザーとは、 AWS アカウント 組織内や社内のビジネスアプリケーションでアクセスを許可する従業員または契約社員です。これらの個人は、社内システムや顧客向けシステムを構築する開発者でも、社内のデータベースシステムやアプリケーションのユーザーでもかまいません。IAM Identity Center でワークフォースユーザーとグループを作成したり、自社の ID ソースにある既存のユーザーやグループに接続して同期したりして、すべてのアプリケーションで使用することができます AWS アカウント 。詳細については、「ID ソースを管理する」を参照してください。

IAM アイデンティティセンターのインスタンスの管理

IAM アイデンティティセンターは、組織インスタンスとアカウントインスタンスの 2 種類のインスタンスをサポートします。組織インスタンスはベストプラクティスです。 AWS アカウント ア

クセスを管理できるのはこのインスタンスだけであり、アプリケーションを本番環境で使用する場合すべてに推奨されます。 AWS Organizations 組織インスタンスは管理アカウントにデプロイされ、 AWS 環境全体のユーザーアクセスを一元的に管理できます。

アカウントインスタンスは、 AWS アカウント 有効化されたインスタンスにバインドされます。IAM Identity Center のアカウントインスタンスは、 AWS 特定の管理対象アプリケーションの個別のデプロイメントをサポートする場合にのみ使用してください。詳細については、「IAM アイデンティティセンターの組織インスタンスとアカウントインスタンスの管理」を参照してください。

複数へのアクセスを管理します。 AWS アカウント

マルチアカウント権限を使用すると、各アカウントを手動で設定しなくても、 AWS アカウント 複数のアカウントにわたる権限を一度に計画して一元的に実装できます。一般的な職務に基づいてアクセス許可を作成したり、セキュリティニーズを満たすカスタム権限を定義したりすることができます。その後、それらの権限をワークフォースユーザーに割り当て、特定のアカウントに対するアクセスを制御できます。

このオプション機能は組織インスタンスでのみ使用できます。お使いの環境でアカウントごとの IAM ロール管理を使用している場合は、両方のシステムを共存させることができます。マルチアカウントアクセス許可を試してみたい場合は、このシステムを限定的に実装することから始め、時間の経過とともに、より多くの環境を移行してこのシステムを使用できます。

アプリケーションへのアクセスの管理

IAM アイデンティティセンターを使用すると、アプリケーションのアクセス管理を簡素化できます。IAM アイデンティティセンターを利用すると、IAM アイデンティティセンターのワークフォースユーザーにアプリケーションへのシングルサインオンのアクセス許可を付与できます。

AWS 管理対象アプリケーション

AWS には Amazon Redshift、Amazon Managed Grafana や Amazon Monitron などの IAM アイデンティティセンターと統合されるアプリケーションが含まれています。これらのアプリケーションでは IAM アイデンティティセンターを使用して、認証、ディレクトリサービス、信頼できる ID の伝播を行うことができます。ユーザーは一貫したシングルサインオンのエクスペリエンスの恩恵を受けます。また、アプリケーションはユーザー、グループ、およびグループメンバーシップに関する共通のビューを共有するため、ユーザーはアプリケーションリソースを他のユーザーと共有する際にも一貫したエクスペリエンスを得ることができます。AWS マネージドアプリケーションを IAM Identity Center と連携するように設定して、関連するアプリケーションコンソール内から直接、または API を介して行うことができます。

カスタマーマネージドアプリケーション

IAM アイデンティティセンターのワークフォースユーザーに、SAML 2.0 による ID フェデレーションをサポートするアプリケーションへのシングルサインオンのアクセス許可を付与できます。Salesforce や Microsoft 365 など、一般的に使用されている SAML 2.0 アプリケーションの多くは IAM アイデンティティセンターと連携し、IAM アイデンティティセンターのコンソールのアプリケーションカタログで利用できます。これはオプション機能で、このようなアプリケーションを使用して IAM アイデンティティセンターでユーザーとグループを作成する場合や、ID ソースとして Microsoft Active Directory ドメインサービスを使用する場合に役立ちます。

アプリケーション間での信頼されたアイデンティティのプロパゲーション

信頼できる ID の伝達により、サービス内のデータへのアクセスを必要とするクエリツールやビジネスインテリジェンス (BI) アプリケーションのユーザーに、効率的なシングルサインオン操作が可能になります。 AWS データアクセス管理はユーザーの ID に基づいているため、管理者はユーザーの既存のユーザーやグループのメンバーシップに基づいてアクセスを許可できます。 AWS サービスやその他のイベントへのユーザーアクセスは、 CloudTrail サービス固有のログとイベントに記録されるため、監査人はユーザーがどのようなアクションをとり、どのリソースにアクセスしたかを把握できます。

AWS ユーザはポータルにアクセスできます。

AWS アクセスポータルは、 AWS アカウント ユーザーが割り当てられたものやアプリケーションすべてにシームレスにアクセスできるようにするシンプルな Web ポータルです。

IAM Identity Center の名称変更

2022 年 7 月 26 日、 AWS シングルサインオンはに名称が変更されました。 AWS IAM Identity Center既存のお客様向けに、名前変更に伴って本ガイド全体で更新された、より一般的な用語の変更の一部を以下の表にまとめました。

旧用語	現在の用語
AWS SSO ユーザーまたは SSO ユーザー	ワークフォースユーザーまたはユーザー
AWS SSO ユーザーポータルまたはユーザーポータル	AWS アクセスポータル
AWS SSO 統合アプリケーション	AWS マネージドアプリケーション

旧用語	現在の用語
AWS SSO ディレクトリ	Identity Center ディレクトリ
AWS SSO ストアまたは AWS SSO アイデンティティストア	IAM Identity Center の使用する Identity Store

次の表は、この名前変更に伴って発生したユーザー、開発者、API リファレンスガイドの該当する名前変更を示しています。

レガシーガイド	現在のガイド
AWS シングルサインオンユーザーガイド	IAM Identity Center ユーザーガイド
AWS シングル・サインオン (SCIM) 実装開発者ガイド	IAM Identity Center SCIM 実装開発者ガイド
AWS シングル・サインオン API リファレンス・ガイド	IAM Identity Center API リファレンス
AWS シングルサインオン ID ストア API リファレンスガイド	Identity Center API リファレンス
AWS シングルサインオン OIDC API リファレンスガイド	IAM Identity Center OIDC API リファレンス
AWS シングル・サインオン・ポータル API リファレンス・ガイド	IAM Identity Center ポータル API リファレンス

レガシー名前空間は変わりません。

`sso` および `identitystore` API 名前空間、および以下の関連名前空間は、下位互換性を保つため変更されていません。

- CLI コマンド
  - `aws configure sso`

  - identitystore
  - sso
  - sso-admin
  - sso-oidc
- AWSSSO と AWSIdentitySync プレフィックスを含む管理ポリシー
- sso と identitystore を含むサービスエンドポイント
- AWS::SSO プレフィックスを含む AWS CloudFormation リソース
- AWSServiceRoleForSSO を含むサービスにリンクされたロール
- sso と singlesignon を含むコンソール URL
- singlesignon を含むドキュメンテーション URL

の有効化 AWS IAM Identity Center

にサインイン AWS Management Console し、IAM Identity Center の組織インスタンスを有効にするには、次のステップを実行します。

1. 以下のいずれかを行って、 AWS Management Consoleにサインインします。
   - 新規ユーザー AWS （ ルートユーザー ） – ルートユーザーを選択し、 AWS アカウント E メールアドレスを入力して、アカウント所有者としてサインインします。次のページでパスワードを入力します。
   - 既に AWS (IAM 認証情報) を使用 – 管理者権限を持つ IAM 認証情報を使用してサインインします。
2. IAM Identity Center コンソールを開きます。
3. [IAM アイデンティティセンターを有効にする] で、[AWS Organizationsで有効にする] を選択します。
4. (オプション) この組織インスタンスに関連付けるタグを追加します。
5. (オプション) 委任管理を設定します。

> **Note**
>
> マルチアカウント環境を使用している場合は、委任管理を設定することをお勧めします。委任管理では、 AWS Organizationsの管理アカウントへのアクセスを必要とするユーザーの数を制限できます。詳細については、「委任された管理」を参照してください。

> **Important**
>
> IAM アイデンティティセンターのアカウントインスタンスを作成する機能は、デフォルトで有効になっています。IAM アイデンティティセンターのアカウントインスタンスには、組織インスタンスで使用できる機能のサブセットが含まれています。サービスコントロールポリシーを使用して、ユーザーがこの機能にアクセスできるかどうかを制御できます。

ファイアウォールやゲートウェイを更新する必要がありますか?

次世代ファイアウォール (NGFW) や Secure Web Gateway (SWG) などのウェブコンテンツフィルタリングソリューションを使用して特定の AWS ドメインまたは URL エンドポイントへのアクセスをフィルタリングする場合は、ウェブコンテンツフィルタリングソリューションの許可リストに次のドメインまたは URL エンドポイントを追加する必要があります。これにより、 AWS アクセスポータルにアクセスできます。

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

ドメインと URL エンドポイントの許可リストに関する考慮事項

AWS アクセスポータル以外の許可リストドメインの影響を理解します。

- AWS アクセスポータルから AWS アカウント、 AWS Management Console、および IAM Identity Center コンソールにアクセスするには、追加のドメインを許可リストに登録する必要があります。 AWS Management Console ドメインのリストについては、AWS Management Console 「入門ガイド」の「トラブルシューティング」を参照してください。
- AWS アクセスポータルから AWS マネージドアプリケーションにアクセスするには、それぞれのドメインを許可リストに登録する必要があります。ガイダンスについては、それぞれのサービスドキュメントを参照してください。
- これらの許可リストは AWS のサービスを対象としています。外部ソフトウェア IdPs (Oktaや などMicrosoft Entra ID) を使用する場合は、許可リストにそのドメインを含める必要があります。

これで IAM アイデンティティセンターを設定する準備ができました。IAM アイデンティティセンターを有効にすると、デフォルトの ID ソースとして Identity Center ディレクトリが自動的に構成されます。これが IAM アイデンティティセンターの使用を開始する最も速い方法です。手順については、「デフォルトの IAM アイデンティティセンターディレクトリを使用してユーザーアクセスを設定する」を参照してください。

IAM アイデンティティセンターが Organizations、ID ソース、IAM ロールとどのように連携するかについて詳しく知りたい場合は、以下のトピックを参照してください。

トピック

前提条件と考慮事項

以下のトピックでは、IAM Identity Center をセットアップするための前提条件とその他の考慮事項について説明します。

を選択する際の考慮事項 AWS リージョン

IAM Identity Center インスタンスは、任意の 1 つのサポート対象で有効に AWS リージョン できます。リージョンを選択するには、ユースケースと企業ポリシーに基づいて優先順位を評価する必要があります。IAM Identity Center からの AWS アカウント およびクラウドアプリケーションへのアクセスは、この選択に依存しません。ただし、 AWS マネージドアプリケーションへのアクセスと ID ソース AWS Managed Microsoft AD として使用する機能は、この選択によって異なります。AWS IAM Identity Center がサポートするリージョンのリストについては、「」の「IAM Identity Center エンドポイントとクォータ」を参照してください。 AWS 全般のリファレンス

を選択するための主な考慮事項 AWS リージョン。

- 地理的位置 – エンドユーザーの大部分に地理的に最も近いリージョンを選択すると、Amazon などの AWS アクセスポータルや AWS マネージドアプリケーションへのアクセスのレイテンシーが低くなります SageMaker Studio。
- AWS マネージドアプリケーションの可用性 – AWS Amazon などのマネージドアプリケーション SageMakerは、サポートする でのみ動作 AWS リージョン できます。使用する AWS マネージドアプリケーションによってサポートされているリージョンで IAM Identity Center を有効にします (複数可) 。多くの AWS マネージドアプリケーションは、IAM Identity Center を有効にしたのと同じリージョンでのみ動作できます。

- デジタル主権 – デジタル主権規制または企業ポリシーでは、特定の の使用が義務付けられている場合があります AWS リージョン。会社の法務部門に相談してください。
- ID ソース – AWS Managed Microsoft AD または AD Connector を ID ソースとして使用している場合、そのホームリージョンは IAM Identity Center を有効に AWS リージョン した と一致する必要があります。
- リージョンはデフォルトで無効になっています。 AWS 最初は、すべての新しい AWS リージョン が AWS アカウント デフォルトで有効になり、ユーザーはどのリージョンでもリソースを自動的に作成できるようになりました。が新しいリージョン AWS を追加すると、その使用はすべてのアカウントでデフォルトで無効になります。デフォルトで無効になっているリージョンに IAM Identity Center をデプロイする場合は、IAM Identity Center へのアクセスを管理するすべてのアカウントでこのリージョンを有効にする必要があります。これは、それらのアカウントでそのリージョンにリソースを作成する予定がない場合でも必要です。

  組織内の現在のアカウントのリージョンを有効にできます。後で追加する可能性のある新しいアカウントに対して、このアクションを繰り返す必要があります。手順については、 ユーザーガイドの「組織内のリージョンを有効または無効にする AWS Organizations 」を参照してください。これらの追加ステップが繰り返し行われないようにするには、デフォルトで有効になっているリージョンに IAM Identity Center をデプロイすることを選択できます。参考までに、以下のリージョンがデフォルトで有効になっています。

  - 米国東部 (オハイオ)
  - 米国東部 (バージニア北部)
  - 米国西部 (オレゴン)
  - 米国西部 (北カリフォルニア)
  - 欧州 (パリ)
  - 南米 (サンパウロ)
  - アジアパシフィック (ムンバイ)
  - 欧州 (ストックホルム)
  - アジアパシフィック (ソウル)
  - アジアパシフィック (東京)
  - 欧州 (アイルランド)
  - 欧州 (フランクフルト)
  - 欧州 (ロンドン)
  - アジアパシフィック (シンガポール)

  - アジアパシフィック (シドニー)
  - カナダ (中部)
  - アジアパシフィック (大阪)
- クロスリージョン呼び出し – 一部のリージョンでは、IAM Identity Center が別のリージョンで Amazon Simple Email Service を呼び出して E メールを送信する場合があります。これらのクロスリージョン呼び出しでは、IAM Identity Center は特定のユーザー属性を他のリージョンに送信します。リージョンの詳細については、「AWS IAM Identity Center リージョンの可用性」を参照してください。

切り替え AWS リージョン

IAM Identity Center リージョンを切り替えるには、現在のインスタンスを削除し、別のリージョンに新しいインスタンスを作成します。既存のインスタンスで AWS マネージドアプリケーションがすでに有効になっている場合は、IAM Identity Center を削除する前に、まずそのアプリケーションを削除する必要があります。ユーザー、グループ、アクセス許可セット、アプリケーション、割り当てを新しいインスタンスで再作成する必要があります。IAM Identity Center アカウントとアプリケーション割り当て APIs を使用して設定のスナップショットを取得し、そのスナップショットを使用して新しいリージョンで設定を再構築できます。また、新しいインスタンスの マネジメントコンソールを使用して、一部の IAM Identity Center 設定を再作成する必要がある場合もあります。IAM Identity Center を削除する手順については、「」を参照してくださいIAM Identity Center 設定を削除する。

IAM Identity Center によって作成された IAM ロールのクォータ

IAM アイデンティティセンターは IAM ロールを作成して、ユーザーにリソースへのアクセス許可を付与します。アクセス許可セットを割り当てると、IAM アイデンティティセンターは、対応する IAM アイデンティティセンター制御の IAM ロールを各アカウントに作成し、アクセス許可セットで指定されたポリシーをそれらのロールに適用します。IAM Identity Center は、 AWS アクセスポータルまたは を使用してロールを管理し、定義した認可されたユーザーがロールを引き受けることを許可します AWS CLI。アクセス権限セットを変更すると、IAM Identity Center は、対応する IAM ポリシーとロールがそれに応じて更新されることを保証します。

で IAM ロールをすでに設定している場合は AWS アカウント、アカウントが IAM ロールのクォータに近づいているかどうかを確認することをお勧めします。アカウントあたりの IAM ロールのデフォルトクォータは 1000 ロールです。詳細については、「IAM オブジェクトクォータ」を参照してください。

クォータに近づいている場合は、クォータの増額をリクエストすることを検討してください。そうしないと、IAM ロールクォータを超えたアカウントにアクセス権限セットをプロビジョニングする際に、IAM Identity Center の問題が発生する可能性があります。クォータ引き上げのリクエストの詳細情報については、「Service Quotas ユーザーガイド」の「クォータ引き上げリクエスト」を参照してください。

> **Note**
>
> すでに IAM アイデンティティセンターを使用しているアカウントの IAM ロールを確認している場合は、ロール名が “AWSReservedSSO_” で始まることに気づくかもしれません。これらは、IAM Identity Center サービスがアカウントに作成したロールであり、アカウントにアクセス権限セットを割り当てたものです。

IAM Identity Center と AWS Organizations

AWS Organizations IAM Identity Center での使用には が推奨されますが、必須ではありません。組織をまだ設定していない場合は、設定する必要はありません。IAM Identity Center を有効にする場合、 でサービスを有効にするかどうかを選択します AWS Organizations。組織を設定すると、組織をセットアップ AWS アカウント する が組織の管理アカウントになります。 AWS アカウント のルートユーザーが組織管理アカウントの所有者になりました。組織に AWS アカウント 招待した追加アカウントはメンバーアカウントです。管理アカウントは、メンバーアカウントを管理する組織リソース、組織単位、およびポリシーを作成します。アクセス許可は管理アカウントによってメンバーアカウントに委任されます。

> **Note**
>
> IAM Identity Center の組織インスタンス AWS Organizationsを作成する で IAM Identity Center を有効にすることをお勧めします。組織インスタンスは IAM アイデンティティセンターのすべての機能をサポートし、一元管理機能を提供するため、おすすめのベストプラクティスです。詳細については、「IAM アイデンティティセンターの組織インスタンスとアカウントインスタンスの管理」を参照してください。

をすでに設定 AWS Organizations していて、組織に IAM Identity Center を追加する場合は、すべての AWS Organizations 機能が有効になっていることを確認してください。組織を作成する際、デフォルトではすべての機能が有効化されています。詳細については、「AWS Organizations ユーザーガイド」の「組織内のすべての機能の有効化」を参照してください。

IAM Identity Center を有効にするには、管理認証情報を持つユーザーまたはルートユーザーとして管理アカウントにサインイン AWS Management Console して、 に AWS Organizations サインインする必要があります (他の管理ユーザーが存在しない場合を除き、推奨されません)。 AWS Organizations メンバーアカウントの管理者認証情報を使用してサインインしている間は、IAM Identity Center を有効にすることはできません。詳細については、「 ユーザーガイド」の AWS 「組織の作成と管理AWS Organizations 」を参照してください。

IAM Identity Center で ID ソースを確認する

IAM Identity Center の ID ソースは、ユーザーやグループがどこで管理されているかを定義します。IAM アイデンティティセンターを有効にしたら、選択した ID ソースを使用していることを確認します。

ID ソースを確認する

1. IAM Identity Center コンソールを開きます。
2. ダッシュボードページの推奨セットアップ手順セクションで、ID ソースの確認を選択します。[設定] を選択し、[ID ソース] タブを選択してもこのページにアクセスできます。
3. 割り当てられた ID ソースを維持したい場合はアクションはありません。変更したい場合は、[アクション] を選択し、[ID ソースを変更] を選択します。

   ID ソースとして以下のいずれかを選択できます。

   Identity Center ディレクトリ

   IAM アイデンティティセンターを初めて有効にすると、IAM アイデンティティセンターディレクトリがデフォルトの ID ソースとして自動的に構成されます。別の外部 ID プロバイダーをまだ使用していない場合は、ユーザーとグループの作成を開始し、それらのアクセスレベルを AWS アカウント およびアプリケーションに割り当てることができます。この ID ソースの使用に関するチュートリアルについては、「デフォルトの IAM アイデンティティセンターディレクトリを使用してユーザーアクセスを設定する」を参照してください。

   アクティブディレクトリ

   AWS Directory Service または のセルフマネージド AWS Managed Microsoft AD ディレクトリを使用してディレクトリ内のユーザーとグループを既に管理している場合はActive Directory (AD)、IAM Identity Center を有効にするときにそのディレクトリを接続することをお勧めします。デフォルトの Identity Center ディレクトリにはユーザーとグループを作成しないでください。IAM Identity Center は、 が提供する接続 AWS Directory Service を使用し

て、Active Directory のソースディレクトリから IAM Identity Center ID ストアにユーザー、グループ、メンバーシップ情報を同期します。詳細については、「Microsoft AD ディレクトリへの接続」を参照してください。

> **Note**
>
> IAM アイデンティティセンターは SAMBA4 ベースの Simple AD を ID ソースとしてサポートしていません。

外部 ID プロバイダー

Okta や などの外部 ID プロバイダー (IdPs) の場合Microsoft Entra ID、IAM Identity Center を使用して、Security Assertion Markup Language (SAML) 2.0 標準 IdPs を通じて から ID を認証できます。SAML プロトコルは、ユーザーやグループについての情報を得るために IdP へクエリする方法は提供していません。IAM アイデンティティセンターがこれらのユーザーやグループを IAM アイデンティティセンターにプロビジョニングして認識する必要があります。IdP が SCIM をサポートしている場合は、System for Cross-domain Identity Management (SCIM) v2.0 プロトコルを使用して、IdP から IAM アイデンティティセンターへのユーザーおよびグループの情報の自動プロビジョニング (同期) を実行できます。それ以外の場合は、ユーザー名、E メールアドレス、グループを IAM アイデンティティセンターに手動で入力して、ユーザーとグループを手動でプロビジョニングできます。

ID ソースの設定手順の詳細については、「」を参照してください入門チュートリアル。

> **Note**
>
> 外部 ID プロバイダーを使用する予定の場合は、IAM アイデンティティセンターではなく外部 IdP が多要素認証 (MFA) 設定を管理することに注意してください。IAM Identity Center の MFA は、外部 での使用はサポートされていません IdPs。詳細については、「ユーザーに MFA を求める」を参照してください。

選択する ID ソースによって、シングルサインオンアクセスを必要とするユーザーとグループを IAM Identity Center が検索する場所が決まります。ID ソースを選択または変更したら、ユーザーを作成または特定し、そのユーザーに AWS アカウントへの管理者権限を割り当てます。

> **Important**
>
> Active Directory もしくは外部の ID プロバイダー (IdP) ですでにユーザーとグループを管理している場合は、IAM Identity Center を有効にして ID ソースを選択するときに、この ID ソースを接続することを検討することをお勧めします。これは、ユーザーやグループをデフォルトの Identity Center ディレクトリに作成して割り当てを行う前に行う必要があります。
>
> すでに IAM Identity Center の 1 つの ID ソースでユーザーとグループを管理している場合、別の ID ソースに変更すると、IAM Identity Center で設定したユーザーとグループの割り当てがすべて削除される可能性があります。この場合、IAM Identity Center の管理ユーザーを含むすべてのユーザーは、 AWS アカウント およびアプリケーションへのシングルサインオンアクセスを失います。詳細については、「ID ソースの変更に関する注意事項」を参照してください。

ID ソースを設定したら、ユーザーまたはグループを検索して AWS アカウント、、クラウドアプリケーション、またはその両方へのシングルサインオンアクセスを許可できます。

入門チュートリアル

組織ごとに 1 つの ID ソースを使用できるため、時間をかけてそれぞれの機能をテストすることが重要です。

このセクションでは、以下のチュートリアルのいずれかを選択して、お好みの ID ソースで IAM アイデンティティセンターをセットアップし、管理ユーザーを作成し、ユーザーにリソースへのアクセスを許可するアクセス許可セットを設定できます。

これらのチュートリアルを開始する前に、IAM Identity Center を有効にします。詳細については、「の有効化 AWS IAM Identity Center」を参照してください。

トピック

- デフォルトの IAM アイデンティティセンターディレクトリを使用してユーザーアクセスを設定する
- Active Directory を ID ソースとして使用する
- Setting up SCIM provisioning between CyberArk and IAM Identity Center
- Google Workspace および IAM アイデンティティセンターによる SAML と SCIM の設定
- IAM アイデンティティセンターを使用して JumpCloud ディレクトリプラットフォームに接続する
- Microsoft Entra ID および IAM アイデンティティセンターによる SAML と SCIM の設定
- Okta および IAM アイデンティティセンターによる SAML と SCIM の設定
- OneLogin と IAM アイデンティティセンター間の SCIM プロビジョニングのセットアップ
- IAM アイデンティティセンターで Ping Identity 製品を使用する

デフォルトの IAM アイデンティティセンターディレクトリを使用してユーザーアクセスを設定する

IAM アイデンティティセンターを初めて有効にすると、Identity Center ディレクトリがデフォルトの ID ソースとして自動的に構成されるため、ID ソースを選択する必要はありません。組織が AWS Directory Service for Microsoft Active Directory、、 などの別の ID プロバイダーを使用している場合Microsoft Entra IDは、デフォルト設定を使用する代わりに、その ID ソースを IAM Identity Center と統合することOktaを検討してください。

目的

このチュートリアルでは、デフォルトディレクトリを ID ソースとして使用し、ユーザーアクセスを設定してテストします。このシナリオでは、IAM アイデンティティセンターですべてのユーザーとグループを管理します。ユーザーは AWS アクセスポータルからサインインします。このチュートリアルは、IAM を初めて使用するユーザー、 AWS または IAM を使用してユーザーとグループを管理しているユーザーを対象としています。次のステップでは、以下を作成します。

- *Nikki Wolf* という名前の管理ユーザー
- ***#####*** という名前のグループ。
- という名前のアクセス許可セット *AdminAccess*

すべてが正しく作成されたことを確認するには、サインインして管理ユーザーのパスワードを設定します。このチュートリアルを完了すると、管理ユーザーを使用して IAM アイデンティティセンターにユーザーを追加したり、アクセス許可セットを追加したり、アプリケーションへの組織的なアクセスを設定したりできます。

IAM アイデンティティセンターをまだ有効にしていない場合は、「の有効化 AWS IAM Identity Center」を参照してください。

開始する前に:

以下のいずれかを行って、 AWS Management Consoleにサインインします。

- 新規ユーザー AWS （ルートユーザー） – AWS アカウント ルートユーザーを選択し、 AWS アカウント E メールアドレスを入力して、アカウント所有者としてサインインします。次のページでパスワードを入力します。
- 既に AWS (IAM 認証情報) を使用 – 管理者権限を持つ IAM 認証情報を使用してサインインします。

IAM Identity Center コンソールを開きます。

ステップ 1: ユーザーを追加する

1. IAM アイデンティティセンターナビゲーションペインで、[ユーザー] を選択し、[ユーザーの追加] を選択します。
2. [ユーザーの詳細を指定] ページで、次の情報を入力します。
   - [ユーザー名] - このチュートリアルでは、*nikkiw* と入力します。

ユーザーを作成するときは、覚えやすいユーザー名を選択してください。ユーザーは AWS アクセスポータルにサインインする際にユーザー名を覚えておく必要があり、後で変更することはできません。

- [パスワード] - [このユーザーにパスワード設定の手順を記載した E メールを送信 (推奨)] を選択します。

  このオプションでは、Amazon Web Services から E メールがユーザーに送信され、件名に「IAM Identity Center への参加の招待 (AWS Single Sign-On の後継) 」と表示されます。E メールは、no-reply@signin.aws または no-reply@login.awsapps.com から送信されます。これらの E メールアドレスを承認済み送信者リストに追加してください。
- [E メールアドレス] - メールを受信できるユーザーの E メールアドレスを入力します。確認のため再入力します。各ユーザーは一意の E メールアドレスを持っている必要があります。
- [名] - ユーザーの名を入力します。このチュートリアルでは、*Nikki* と入力します。
- [姓] - ユーザーの姓を入力します。このチュートリアルでは、*Wolf* と入力します。
- [表示名] - デフォルト値は、ユーザーの名と姓です。表示名を変更したい場合は、別の名前を入力できます。表示名はサインインポータルとユーザーリストに表示されます。
- 必要に応じてオプション情報を入力します。このチュートリアルでは使用されないので、後で変更できます。

3. [次へ] をクリックします。[ユーザーをグループに追加] ページが表示されます。*Nikki* に直接アクセス許可を与えるのではなく、管理者のアクセス許可を割り当てるグループを作成します。

   [グループを作成] を選択する

   新しいブラウザタブで [グループの作成] ページが開きます。

   a. [グループの詳細] の [グループ名] に、グループの名前を入力します。グループのロールを識別するグループ名を使用することをおすすめします。このチュートリアルでは、*Admin team*と入力します。
   b. [グループを作成] を選択する
   c. [グループ] ブラウザータブを閉じて、[ユーザーを追加] ブラウザタブに戻ります。
4. [グループ] 領域で、[更新] ボタンを選択します。*#####*グループがリストに表示されます。

   ##### の横にあるチェックボックスを選択し、次へ を選択します。
5. [ユーザーの確認と追加] ページで、次のことを確認します。

   - 主要情報は意図したとおりに表示されます。

- グループには、作成したグループに追加されたユーザーが表示されます。

変更するには、[Edit] (編集) を選択します。すべての情報が正しければ、[ユーザーを追加] を選択します。

ユーザーが追加されたことを知らせる通知メッセージが表示されます。

次に、*#####*グループの管理アクセス許可を追加して、*Nikki* がリソースにアクセスできるようにします。

ステップ 2: 管理者アクセス許可を追加する

1. IAM アイデンティティセンターのナビゲーションペインの [マルチアカウントのアクセス許可] で、[AWS アカウント] を選択します。
2. [AWS アカウント] ページの[組織構造] には、自分の組織とその下のアカウントが階層内で表示されます。管理アカウントのチェックボックスを選択し、ユーザーまたはグループの割り当てを選択します。
3. [ユーザーとグループを割り当てる] のワークフローが表示されます。これは、3 つのステップから構成されています。

   a. [ステップ 1: ユーザーとグループの選択] では、作成した*#####*グループを選択します。次いで、[次へ] を選択します。

   b. [ステップ 2: アクセス許可セットの選択] では、[許可セットを作成] を選択します。新しいタブが開き、アクセス許可セットを作成するための 3 つのサブステップが順を追って表示されます。

      i. [ステップ 1: 許可セットタイプを選択] では、以下を完了します。

         - [許可セットのタイプ] で、[事前定義された許可セット] を選択します。
         - 事前定義されたアクセス許可セット のポリシーで、 を選択しますAdministratorAccess。

      [次へ] をクリックします。

      ii. [ステップ 2: 許可セットの詳細を指定] では、デフォルト設定のままで、[次へ] を選択します。

デフォルト設定では、セッション時間を 1 時間に設定した という名前*AdministratorAccess*のアクセス許可セットが作成されます。アクセス許可セットの名前を変更するには、アクセス許可セット名フィールドに新しい名前を入力します。

iii. ステップ 3: を確認して作成する で、アクセス許可セットタイプが AWS 管理ポリシーを使用していることを確認しますAdministratorAccess。[作成] を選択します。[アクセス許可セット] ページに、アクセス許可セットが作成されたことを知らせる通知が表示されます。この時点で、ウェブブラウザでこのタブを閉じてもかまいません。

[ユーザーとグループを割り当てる] ブラウザタブでは、[ステップ 2: 許可セットを選択] でアクセス許可セットの作成ワークフローを開始した状態のままになっています。

[アクセス許可セット] 領域で、[更新] ボタンを選択します。作成した*AdministratorAccess*アクセス許可セットがリストに表示されます。そのアクセス許可セットのチェックボックスを選択し、次へ を選択します。

c. ステップ 3: 割り当てを確認して送信 ページで、*######*グループが選択され、*AdministratorAccess*アクセス許可セットが選択されていることを確認してから、送信 を選択します。

ページが更新され、 AWS アカウント が設定されているというメッセージが表示されます。プロセスが完了するまで待ちます。

AWS アカウント ページに戻ります。が再プロビジョニングされ、更新されたアクセス許可セットが適用され AWS アカウント たことを通知する通知メッセージ。

お疲れ様でした。

最初のユーザー、グループ、アクセス許可セットが正常に設定されました。

このチュートリアルの次の部分では、管理者認証情報を使用して アクセスポータルにサインインして *Nikki* の AWS アクセスをテストし、パスワードを設定します。すぐにコンソールからサインアウトします。

ステップ 3: ユーザーアクセスのテスト

これで *Nikki Wolf* は組織のユーザーになりました。Nikki Wolf は、サインインして、アクセス許可セットに従ってアクセス許可が付与されているリソースにアクセスできます。ユーザーが正しく設定されていることを確認するために、次のステップでは *Nikki* の認証情報を使用してサインインし、パスワードを設定します。ステップ 1 でユーザー *Nikki Wolf* を追加したときに、*Nikki* にパスワード設定の手順が記載された E メールを受信するように選択しました。この E メールを開いて、以下の操作を行います。

1. E メール内の [招待を承認] リンクを選択して招待を承諾します。

   > **Note**
   >
   > E メールには、*Nikki* のユーザー名と、組織へのサインインに使用する AWS アクセスポータル URL も含まれています。将来使用するためにこの情報を記録します。

   Nikki のパスワードを設定できる [新規ユーザーのサインアップ] ページが表示されます。
2. *Nikki* のパスワードを設定すると、[サインイン] ページに移動します。*nikkiw* と入力して [次へ] を選択し、*Nikki* のパスワードを入力して [サインイン] を選択します。
3. AWS アクセスポータルが開き、アクセスできる組織とアプリケーションが表示されます。

   組織を選択して のリストに展開 AWS アカウント し、アカウントを選択して、アカウントのリソースにアクセスするために使用できるロールを表示します。

   各アクセス許可セットには、ロールキー またはアクセスキー の 2 つの管理方法があります。

   - ロール 、例えば *AdministratorAccess* - を開きます AWS Console Home。
   - アクセスキー - AWS CLI または および AWS SDK で使用できる認証情報を提供します。自動的に更新される短期認証情報または短期アクセスキーのいずれかを使用するための情報が含まれます。詳細については、「AWS CLI または AWS SDKs」を参照してください。
4. ロールリンクを選択して、 にサインインします AWS Console Home。

サインインし、 AWS Console Home ページに移動します。コンソールを表示して、期待どおりのアクセス許可があることを確認します。

次のステップ

IAM アイデンティティセンターで管理ユーザーを作成したため、次のことができるようになりました。

- アプリケーションを割り当てる
- 他のユーザーを追加する
- ユーザーをアカウントに割り当てる
- 追加のアクセス許可セットを設定する

> **Note**
>
> 同じユーザーに複数のアクセス許可セットを割り当てることもできます。最小権限の権限を適用するというベストプラクティスに従うには、管理ユーザーを作成した後に、より制限の厳しいアクセス権限セットを作成して同じユーザーに割り当てます。これにより、管理アクセス許可ではなく、必要なアクセス許可のみ AWS アカウント を使用して にアクセスできます。

ユーザーが自分のアカウントをアクティブ化するための招待を受け入れ、 AWS アクセスポータルにサインインすると、ポータルに表示される項目は、割り当てられている AWS アカウント、ロール、およびアプリケーションのみです。

> **Important**
>
> ユーザーに対して多要素認証 (MFA) を有効にすることを強くお勧めします。詳細については、「Identity Center ユーザー用の多要素認証」を参照してください。

Active Directory を ID ソースとして使用する

Active Directory (AD) で AWS Directory Service を使用する AWS Managed Microsoft AD ディレクトリまたは自己管理型ディレクトリのいずれかでユーザーを管理している場合は、それらのユーザーと連携するように IAM アイデンティティセンターの ID ソースを変更できます。IAM アイデンティティセンターを有効にして ID ソースを選択するときは、この ID ソースを接続することを検討することをお勧めします。デフォルトの Identity Center ディレクトリでユーザーやグループを作成する前に接続しておくと、後から ID ソースを変更する場合に必要となる追加の設定を回避できます。

Active Directory を ID ソースとして使用するには、設定は次の前提条件を満たす必要があります。

- AWS Managed Microsoft AD を使用している場合は、AWS Managed Microsoft AD ディレクトリが設定されている場所と同じ AWS リージョン で IAM Identity Center を有効にする必要があります。IAM Identity Center では、割り当てデータに関するディレクトリと同じリージョンに保存されます。IAM Identity Center を管理するには、IAM Identity Center が設定されているリージョンに切り替える必要がある場合があります。また、AWS のアクセスポータルでは、ディレクトリと同じアクセス URL が使用されます。
- 管理アカウントにある Active Directory を使用してください。

  既存の AD コネクタまたは AWS Managed Microsoft AD ディレクトリが AWS Directory Service に設定されており、AWS Organizations 管理アカウント内に存在する必要があります。一度に接続できる AD Connector ディレクトリは 1 つか、ディレクトリは AWS Managed Microsoft AD 1 つだけです。複数のドメインやフォレストをサポートする必要がある場合は、AWS Managed Microsoft AD を使用してください。詳細については、以下を参照してください。

  - のディレクトリを IAM Identity Center AWS Managed Microsoft AD に接続する
  - Active Directory の自己管理型ディレクトリを IAM Identity Center に接続する
- 委任された管理者アカウントにある Active Directory を使用してください。

  IAM アイデンティティセンター委任管理者を有効にし、IAM アイデンティティセンターの ID ソースとして Active Directory を使用する予定の場合は、委任された管理者アカウントにある AWS ディレクトリに設定された既存の AD Connector または AWS Managed Microsoft AD ディレクトリを使用できます。

  IAM Identity Center ID ソースを他のソースから Active Directory に変更するか、Active Directory から他のソースに変更する場合、そのディレクトリは IAM Identity Center 委任管理者メンバーアカウント (存在する場合) に存在する (所有されている) 必要があります。それ以外の場合は、管理アカウントに含まれている必要があります。

このチュートリアルでは、Active Directory を IAM アイデンティティセンターの ID ソースとして使用するための基本設定について説明します。

ステップ 1: Active Directory に接続し、ユーザーを指定する

すでに Active Directory を使用している場合は、以下のトピックがディレクトリを IAM アイデンティティセンターに接続する準備に役立ちます。

> **Note**
>
> セキュリティのベストプラクティスとして、多要素認証を有効にすることを強くお勧めします。Active Directory 内の AWS Managed Microsoft AD ディレクトリまたは自己管理型ディレクトリを接続する予定で、RADIUS MFA を AWS Directory Service と一緒に使用していない場合は、IAM Identity Center で MFA を有効にします。

AWS Managed Microsoft AD

1. Microsoft AD ディレクトリへの接続 のガイダンスを確認してください。
2. 「のディレクトリを IAM Identity Center AWS Managed Microsoft AD に接続する」の手順を実行します。
3. 管理者権限を付与したいユーザーを IAM Identity Center と同期するように Active Directory を設定します。詳細については、「管理ユーザーを IAM Identity Center と同期する」を参照してください。

Active Directory 内の自己管理型ディレクトリ

1. Microsoft AD ディレクトリへの接続 のガイダンスを確認してください。
2. 「Active Directory の自己管理型ディレクトリを IAM Identity Center に接続する」の手順を実行します。
3. 管理者権限を付与したいユーザーを IAM Identity Center と同期するように Active Directory を設定します。詳細については、「管理ユーザーを IAM Identity Center と同期する」を参照してください。

ステップ 2: 管理ユーザーを IAM アイデンティティセンターと同期する

ディレクトリを IAM Identity Center に接続したら、管理権限を付与するユーザーを指定し、そのユーザーをディレクトリから IAM Identity Center に同期できます。

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. 「設定」ページで「ID ソース」タブを選択し、「アクション」を選択し、「同期を管理」を選択します。
4. [同期の管理] ページで、[ユーザー] タブを選択し、[ユーザーとグループの追加] を選択します。

5. [ユーザー] タブの [ユーザー] に正確なユーザー名を入力し、[追加] を選択します。
6. [追加されたユーザーとグループ] で、次の操作を行います。

   a. 管理者権限を付与するユーザーが指定されていることを確認します。
   b. ユーザー名の左側にあるチェックボックスをオンにします。
   c. [Submit] (送信) を選択します。
7. [同期の管理] ページで、指定したユーザーが同期対象のユーザーリストに表示されます。
8. ナビゲーションペインで [Users (ユーザー)] を選択します。
9. 「ユーザー」ページでは、指定したユーザーがリストに表示されるまでに時間がかかる場合があります。ユーザーリストを更新するには、[更新] アイコンをクリックします。

この時点では、ユーザーは管理アカウントにアクセスできません。このアカウントへの管理アクセスを設定するには、管理アクセス権限セットを作成し、そのアクセス権限セットにユーザを割り当てます。詳細については、「アクセス権限セットを作成します。」を参照してください。

Setting up SCIM provisioning between CyberArk and IAM Identity Center

IAM Identity Center は、CyberArk Directory Platform から IAM Identity Center へのユーザ情報の自動プロビジョニン グ (同期) をサポートしています。このプロビジョニングでは、クロスドメインアイデンティティ管理システム (SCIM) v2.0 プロトコルを使用します。この接続を CyberArk で設定するには、IAM Identity Center SCIM エンドポイントとアクセストークンを使用します。SCIM 同期を設定すると、CyberArk のユーザー属性と IAM Identity Center の名前付き属性のマッピングが作成されます。これにより、IAM Identity Center と CyberArk の間で、期待される属性が一致します。

このガイドは 2021 年 8 月時点の CyberArk をベースとしています。新しいバージョンでは、手順が異なる場合があります。このガイドには、SAML によるユーザー認証の設定に関するいくつかの注意事項が記載されています。

> **Note**
>
> SCIM のデプロイを開始する前に、まず 自動プロビジョニングを使用する際の注意事項 を確認することをお勧めします。そして、次のセクションで残りの注意事項を確認します。

トピック

前提条件

開始する前に、以下の準備が必要です。

- CyberArk のサブスクリプションまたは無料トライアル。無料トライアルにサインアップするには、CyberArk にアクセスしてください。
- IAM Identity Center 対応アカウント (無料)。詳細については、「IAM Identity Center の有効化」を参照してください。
- 「CyberArkIAM ID Centerのドキュメント」で説明されている、CyberArk アカウントから IAM アイデンティティセンターへの SAML 接続。
- IAM Identity Center コネクターを、 AWS アカウントへのアクセスを許可したいロール、ユーザー、組織に関連付けます。

SCIM に関する注意事項

IAM Identity Center に CyberArk のフェデレーションを使用する場合の注意事項を以下に示します。

- アプリケーションプロビジョニングセクションでマッピングされたロールだけが IAM Identity Center に同期されます。
- プロビジョニングスクリプトはデフォルトの状態でのみサポートされており、変更すると SCIM のプロビジョニングに失敗する可能性があります。
  - 同期できる電話番号属性は 1 つだけです。デフォルトは「仕事用の電話」です。
- CyberArk IAM Identity Center アプリケーションのロールマッピングを変更すると、以下のような動作になります。
  - ロール名を変更しても、IAM Identity Center のグループ名は変更されません。

- グループ名が変更された場合、IAM Identity Center では新しいグループが作成されます。古いグループは残りますが、メンバーはいません。
- ユーザーの同期とプロビジョニング解除の動作は、CyberArk IAM Identity Center アプリケーションから設定できますので、組織に合った動作を設定してください。オプションは次の通りです。
  - Identity Center ディレクトリ内の同じプリンシパル名のユーザーを上書きする (しない)。
  - ユーザーが CyberArk のロールから削除されたときに、IAM Identity Center からユーザーを非プロビジョニングします。
  - ユーザー動作のプロビジョニングの解除 - 無効化または削除。

ステップ 1: IAM Identity Center でプロビジョニングを有効にする

この最初のステップでは、IAM Identity Center コンソールを使用して、自動プロビジョニングを有効にします。

IAM Identity Center で自動プロビジョニングを有効にするには

1. 前提条件が整ったら、IAM Identity Center コンソールを開きます。
2. 左側のナビゲーションペインの [Settings] (設定) を選択します。
3. [設定] ページで、[自動プロビジョニング] 情報ボックスを探し、[有効化] を選択します。これにより、すぐに IAM Identity Center の自動プロビジョニングが有効になり、必要なエンドポイントとアクセストークンの情報が表示されます。
4. [Inbound automatic provisioning] (インバウンド自動プロビジョニング) ダイアログボックスで、以下のオプションの値をそれぞれコピーします。これらは、後で IdP でプロビジョニングを設定する際に貼り付ける必要があります。
   a. SCIM エンドポイント
   b. アクセストークン
5. [Close] (閉じる) を選択します。

IAM Identity Center でプロビジョニングを設定したので、CyberArk IAM Identity Center アプリケーションを使用して残りのタスクを完了する必要があります。これらのステップについて、次の手順で説明します。

ステップ 2: CyberArk でプロビジョニングを設定する

CyberArk IAM Identity Center アプリケーションで以下の手順を使用して、IAM Identity Center によるプロビジョニングを有効にします。この手順では、CyberArk IAM Identity Center アプリケーションが Web Apps (ウェブアプリケーション)で CyberArk 管理コンソールに追加されていることを前提としています。まだ実行していない場合は、「前提条件」を参照してから、この手順を実行して SCIM プロビジョニングを設定してください。

CyberArk でプロビジョニングを設定するには

1. CyberArk の SAML 構成の一部として追加した CyberArk IAM Identity Center アプリケーションを開きます（アプリ>ウェブアプリ）。前提条件 を参照してください。
2. [IAM Identity Center] アプリケーションを選択し、[プロビジョニング] セクションに移動します。
3. [Enable provisioning for this application] (このアプリケーションのプロビジョニングを有効にする) にチェックを入れ、[Live Mode] (ライブモード) を選択します。
4. 前の手順で、IAM Identity Center から [SCIM エンドポイント] の値をコピーしました。その値を [SCIM サービスのURL] フィールドに貼り付け、CyberArk IAM Identity Center のアプリケーションで、[認証タイプ] を [認証ヘッダー] に設定します。URL の末尾にあるスラッシュを削除してください。
5. [Header Type] (ヘッダータイプ) を [Bearer Token] (ベアラートークン) に設定します。
6. 前の手順で、IAM Identity Center の [アクセストークン] の値をコピーしました。その値を CyberArk IAM Identity Center アプリケーションの「ベアラートークン」フィールドに貼り付けます。
7. [Verify] (検証) をクリックすると、設定をテストして、適用します。
8. [同期オプション] で、CyberArk からのアウトバウンドプロビジョニングを動作させるための正しい動作を選択します。似たようなプリンシパル名を持つ既存の IAM Identity Center ユーザーを上書きする (または上書きしない) かどうか、プロビジョニング解除の動作を選択できます。
9. [ロールマッピング] では、[名前] フィールドにある CyberArk ロールから [送信先グループ] にある IAM Identity Center グループへのマッピングを設定します。
10. 完了したら、下部の [Save] (保存) をクリックします。
11. ユーザーが IAM Identity Center に正常に同期されたことを確認するには、IAM Identity Center コンソールに戻り、[ユーザー] を選択します。CyberArk から同期されたユーザーは、[ユーザー] ページに表示されます。これらのユーザーは、アカウントに割り当てられ、IAM Identity Center で接続できるようになりました。

(オプション) ステップ 3: IAM Identity Center でのアクセスコントロール (ABAC) のために CyberArk でユーザー属性を設定する

これは、 AWS リソースへのアクセスを管理するために IAM Identity Center の属性を設定する CyberArk場合のオプションの手順です。CyberArk で定義した属性は、SAML アサーションで IAM Identity Center に渡されます。その後、IAM Identity Center でアクセス権限セットを作成し、CyberArk から渡された属性に基づいてアクセスを管理します。

この手順を始める前に、最初に アクセスコントロールの属性 機能を有効にしておく必要があります。これを行う方法については、「アクセスコントロールのための属性の有効化と設定」を参照してください。

IAM Identity Center でのアクセスコントロールに使用される CyberArk の属性の有効化と設定

1. CyberArk の SAML 構成の一部としてインストールした CyberArk IAM Identity Center アプリケーションを開きます（ アプリ>ウェブアプリ ）。
2. [SAML Response] (SAML レスポンス) オプションに移動します。
3. [Attributes] (属性) では、以下のようなロジックでテーブルに関連する属性を追加します。
   a. [属性名] は、CyberArk のオリジナルの属性名です。
   b. [属性値] は、IAM Identity Center への SAML アサーションで送信される属性名です。
4. [保存] を選択します。

(オプション) アクセスコントロールの属性を渡す

IAM Identity Center の アクセスコントロールの属性 機能をオプションで使用して、Name 属性を `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` に設定した `Attribute` 要素を渡すことができます。この要素を使用すると、SAML アサーションでセッションタグとして属性を渡すことができます。セッションタグの詳細については、「IAM ユーザーガイド」の「 AWS STSでのタグ付けの規則 」 を参照してください。

属性をセッションタグとして渡すには、タグの値を指定する `AttributeValue` 要素を含めます。例えば、タグのキーバリューのペア `CostCenter = blue` を渡すには、次のような属性を使用します。

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

```
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

複数の属性を追加する必要がある場合は、各タグに個別の `Attribute` 要素を含めます。

Google Workspace および IAM アイデンティティセンターによる SAML と SCIM の設定

組織が を使用している場合はGoogle Workspace、 から IAM Identity Center Google Workspaceにユーザーとグループを統合して、 AWS リソースへのアクセスを許可できます。この統合は、IAM Identity Center アイデンティティソースをデフォルトの IAM Identity Center アイデンティティソースから に変更することで実現できますGoogle Workspace。

Google Workspace のユーザー情報は、クロスドメイン ID 管理システム (SCIM) v2.0 プロトコルを使用して IAM アイデンティティセンターに同期されます。Google Workspace で、この接続を IAM アイデンティティセンター用 SCIM エンドポイントと IAM アイデンティティセンターのベアラートークンを使用して設定します。SCIM 同期を設定すると、Google Workspace のユーザー属性と IAM Identity Center の名前付き属性のマッピングが作成されます。このマッピングは、IAM アイデンティティセンターと Google Workspace の間で、期待されるユーザー属性を照合します。そのためには、Google Workspace を IAM ID プロバイダーと IAM アイデンティティセンターID プロバイダーとして設定する必要があります。

目的

このチュートリアルのステップは、 Google Workspaceと 間の SAML 接続を確立する手順に役立ちます AWS。後で、SCIM を使用して Google Workspace のユーザーを同期します。すべてが正しく設定されていることを確認するには、設定ステップを完了すると、Google Workspaceユーザーとしてサインインし、 AWS リソースへのアクセスを確認します。このチュートリアルは小規模 Google Workspace ディレクトリのテスト環境に基づいていることに注意してください。グループや組織単位などのディレクトリ構造は含まれていません。このチュートリアルを完了すると、ユーザーは認証情報を使用して AWS アクセスポータルにアクセスできますGoogle Workspace。

> **Note**
>
> Google Workspace の無料トライアルにサインアップするには、Google's Web サイトの Google Workspace にアクセスしてください。

IAM アイデンティティセンターをまだ有効にしていない場合は、「の有効化 AWS IAM Identity Center」を参照してください。

考慮事項

- Google Workspace と IAM Identity Center の間で SCIM プロビジョニングを設定する前に、まずを確認することをお勧めします自動プロビジョニングを使用する際の注意事項。
- からの SCIM 自動同期Google Workspaceは現在、ユーザープロビジョニングに制限されています。現時点では、グループの自動プロビジョニングはサポートされていません。グループは、AWS CLI Identity Store の create-group コマンドまたは AWS Identity and Access Management (IAM) API を使用して手動で作成できますCreateGroup。または、ssosync を使用してGoogle Workspaceユーザーとグループを IAM Identity Center に同期することもできます。
- すべての Google Workspace ユーザーにおいて、[名]、[姓]、[ユーザー名]、[表示名] の値を指定する必要があります。
- 各 Google Workspace ユーザーには、E メールアドレスや電話番号などのデータ属性ごとに 1 つの値のみが割り当てられます。複数の値を持つユーザーは同期に失敗します。属性に複数の値を持つユーザーがいる場合は、IAM アイデンティティセンターでユーザーをプロビジョニングする前に、重複する属性を削除してください。例えば、同期できる電話番号属性は 1 つだけです。デフォルトの電話番号属性は「勤務先の電話」なので、ユーザーの電話番号が自宅の電話でも携帯電話でも、「勤務先の電話」属性を使用してユーザーの電話番号を保存します。
- ユーザーが IAM Identity Center で無効化されていても、Google Workspace で有効化されていれば、属性は引き続き同期されます。
- Identity Center ディレクトリに同じユーザー名とパスワードを持つ既存のユーザーがいる場合、そのユーザーは の SCIM を使用して上書きされ、同期されますGoogle Workspace。
- ID ソースを変更する場合は、他にも考慮事項があります。詳細については、「the section called "IAM Identity Center から外部 IdP への変更"」を参照してください。

ステップ 1: Google Workspace: SAML アプリケーションを設定する

1. スーパー管理者権限を持つアカウントを使用して、管理者Googleコンソールにサインインします。
2. Google 管理コンソール の左側のナビゲーションパネルで、アプリ を選択し、ウェブおよびモバイルアプリ を選択します。
3. アプリの追加ドロップダウンリストで、アプリの検索 を選択します。

4. 検索ボックスに「Amazon Web Services」と入力し、リストから「Amazon Web Services (SAML) アプリ」を選択します。
5. Google ID プロバイダーの詳細 - Amazon Web Services ページで、次のいずれかを実行できます。

   a. IdP メタデータをダウンロードします。

   b. SSO URL、エンティティ ID URL、および証明書情報をコピーします。

   ステップ 2 では、XML ファイルまたは URL 情報のいずれかが必要です。
6. Google 管理者コンソールの次のステップに進む前に、このページを開いたままにして、IAM Identity Center コンソールに移動します。

ステップ 2: IAM Identity Center と Google Workspace: IAM Identity Center アイデンティティソースを変更し、SAML ID プロバイダーGoogle Workspaceとして設定する

1. 管理者権限を持つロールを使用して IAM Identity Center コンソールにサインインします。
2. 左側のナビゲーションペインの [Settings] (設定) を選択します。
3. [設定] ページで [アクション] タブを選択し、[ID ソースを変更] を選択します。

   - IAM Identity Center を有効にしていない場合は、IAM アイデンティティセンターを有効にする「」で詳細を確認してください。IAM Identity Center を初めて有効化してアクセスすると、ダッシュボードが表示され、ID ソースの選択を選択できます。
4. [ID ソースを選択] ページで [外部 ID プロバイダー] を選択したら、[次へ] を選択します。
5. [外部 ID プロバイダーの設定] ページが開きます。このページとステップ 1 のGoogle Workspace ページを完了するには、以下を完了する必要があります。

   - IAM Identity Center コンソールの ID プロバイダーメタデータセクションで、次のいずれかを実行する必要があります。

     i. IAM Identity Center Google コンソールで IdP SAML メタデータとして SAML メタデータ IdPをアップロードします。

     ii. Google SSO URL をコピーして IdP サインイン URL フィールドに貼り付け、Google発行者 URL を IdP 発行者 URL フィールドに貼り付け、Google証明書 を IdP 証明書 としてアップロードします。

6. IAM Identity Center コンソールの Identity Provider metadata セクションでGoogleメタデータを指定したら、 AWS アクセスポータルのサインイン URL 、IAM Identity Assertion Consumer Service (ACS) URL 、および IAM Identity Center 発行者 URL をコピーします。これらのURLs、次のステップのGoogle管理者コンソールで指定する必要があります。
7. IAM Identity Center コンソールでページを開いたままにして、Google管理者コンソールに戻ります。Amazon Web Services - サービスプロバイダーの詳細ページに移動する必要があります。[Continue] (続行) をクリックします。
8. サービスプロバイダーの詳細ページで、ACS URL 、エンティティ ID 、開始 URL の値を入力します。これらの値は、前のステップでコピーし、IAM Identity Center コンソールで確認できます。

   - IAM Identity Center Assertion Consumer Service (ACS) URL を ACS URL フィールドに貼り付けます。
   - IAM Identity Center 発行者 URL をエンティティ ID フィールドに貼り付けます。
   - AWS アクセスポータルのサインイン URL を開始 URL フィールドに貼り付けます。
9. サービスプロバイダーの詳細ページで、次のように名前 ID のフィールドに入力します。

   - [名前 ID 形式] で、[E メール] を選択します。
   - [名前 ID] で、[基本情報] > [プライマリ E メールアドレス] を選択します。
10. [Continue] を選択します。
11. 属性マッピングページの属性 で、マッピングの追加 を選択し、Googleディレクトリ属性 でこれらのフィールドを設定します。

    - `https://aws.amazon.com/SAML/Attributes/RoleSessionName` アプリ属性 で、属性から「基本情報」、「プライマリ E Google Directory メール」のフィールドを選択します。
    - `https://aws.amazon.com/SAML/Attributes/Role` アプリ属性 で、任意のGoogle Directory属性 を選択します。Google ディレクトリ属性は、部門 である可能性があります。
12. [終了] を選択します
13. IAM Identity Center コンソールに戻り、次へ を選択します。確認と確認ページで情報を確認し、表示されたスペースに ACCEPT と入力します。[Change identity source] (ID ソースの変更) を選択します。

これで、ユーザーが IAM Identity Center にプロビジョニングGoogle Workspaceできるように、 で Amazon Web Services アプリを有効にする準備が整いました。

ステップ 3: Google Workspace: アプリケーションを有効にする

1. Google 管理コンソールに戻り、アプリケーション、ウェブ、モバイルアプリケーション で AWS IAM Identity Center を見つけます。
2. ユーザーアクセス の横にあるユーザーアクセスパネルで、下矢印を選択してユーザーアクセスを展開し、サービスステータスパネルを表示します。
3. サービスステータスパネルで、すべてのユーザーに対してオンを選択し、保存を選択します。

> **Note**
>
> 最小特権の原則を維持するために、このチュートリアルを完了したら、すべての のサービスステータスを OFF に変更することをお勧めします。 へのアクセスが必要なユーザーのみが、サービスを有効にする AWS 必要があります。Google Workspace グループまたは組織単位を使用して、ユーザーの特定のサブセットへのアクセス権をユーザーに付与できます。

ステップ 4: IAM アイデンティティセンター: IAM アイデンティティセンターの自動プロビジョニングを設定する

1. IAM アイデンティティセンターコンソールに戻ります。
2. [設定] ページで、[自動プロビジョニング] 情報ボックスを探し、[有効化] を選択します。これにより、すぐに IAM Identity Center の自動プロビジョニングが有効になり、必要なエンドポイントとアクセストークンの情報が表示されます。
3. [Inbound automatic provisioning] (インバウンド自動プロビジョニング) ダイアログボックスで、以下のオプションの値をそれぞれコピーします。このチュートリアルのステップ 5 では、これらの値を入力して、 で自動プロビジョニングを設定しますGoogle Workspace。

   - SCIM エンドポイント
   - アクセストークン

   > **Warning**
   >
   > SCIM エンドポイントとアクセストークンを取得できるのは今回だけです。先に進む前に、必ずこれらの値をコピーしてください。

4. [閉じる] を選びます。

IAM Identity Center コンソールでプロビジョニングを設定したので、次のステップでは で自動プロビジョニングを設定しますGoogle Workspace。

ステップ 5: Google Workspace: 自動プロビジョニングを設定する

1. Google 管理コンソールと AWS IAM Identity Center アプリケーションに戻ります。アプリケーション、ウェブ、モバイルアプリケーション にあります。 [自動プロビジョニング] セクションで、[自動プロビジョニングの設定] を選択します。
2. 前の手順では、IAM Identity Center コンソールでアクセストークン値をコピーしました。アクセストークンフィールドにその値を貼り付け、続行 を選択します。また、前の手順では、IAM Identity Center コンソールで SCIM エンドポイント値をコピーしました。その値を [エンドポイント URL] フィールドに貼り付けます。URL の末尾にあるスラッシュを削除して、[続行]を選択します。
3. すべての必須の IAM アイデンティティセンター属性 (* の付いた属性) が Google Cloud Directory 属性にマップされていることを確認します。そうでない場合は、下矢印を選択して適切な属性にマップします。[Continue] を選択します。
4. 「プロビジョニングスコープ」セクションで、Google Workspaceディレクトリを持つグループを選択して、Amazon Web Services アプリへのアクセスを提供できます。このステップをスキップして [続行] を選択します。
5. プロビジョニング解除セクションでは、ユーザーからアクセスを削除するさまざまなイベントへの対応方法を選択できます。状況ごとに、プロビジョニング解除を開始するまでの時間を指定できます。

   - 24 時間以内
   - 1 日後
   - 7 日後
   - 30 日後

   それぞれの状況には、アカウントのアクセスを一時停止するタイミングとアカウントを削除するタイミングがあります。

> **Tip**
>
> ユーザーのアカウントを削除するまでの時間は、必ずユーザーのアカウントを停止するよりも長く設定してください。

6. [Finish] を選択します。Amazon Web Services アプリページに戻ります。
7. 自動プロビジョニングセクションで、トグルスイッチをオンにして、非アクティブ からアクティブに変更します。

> **Note**
>
> IAM Identity Center がユーザーに対して有効になっていない場合、アクティベーションスライダーは無効になります。[ユーザーアクセス] を選択し、アプリをオンにしてスライダーを有効にします。

8. 確認ダイアログボックスで [オンにする] をクリックします。
9. ユーザーが IAM Identity Center と正常に同期されたことを確認するには、IAM Identity Center コンソールに戻り、[ユーザー] を選択します。[ユーザー] ページには、SCIM によって作成された Google Workspace ディレクトリのユーザーが一覧表示されます。ユーザーがまだリストに表示されていない場合は、プロビジョニングがまだ進行中である可能性があります。プロビジョニングには最長で 24 時間かかることがありますが、ほとんどの場合、数分以内に完了します。ブラウザウィンドウは数分おきに更新してください。

   ユーザーを選択し、その詳細を表示します。情報はGoogle Workspaceディレクトリ内の情報と一致する必要があります。

> **お疲れ様でした。**
>
> Google Workspace と の間の SAML 接続を正常にセットアップ AWS し、自動プロビジョニングが機能していることを検証しました。[IAM Identity Center] でこれらのユーザーをアカウントおよびアプリケーションに割り当てることができるようになりました。このチュートリアルでは、次のステップで、管理アカウントへの管理アクセス許可を付与して、ユーザーの 1 人を IAM アイデンティティセンター管理者として指定しましょう。

ステップ 6: IAM Identity Center: Google Workspaceユーザーに アカウントへのアクセスを許可する

1. IAM Identity Center コンソールに戻ります。IAM アイデンティティセンターのナビゲーションペインの [マルチアカウントのアクセス許可] で、[AWS アカウント] を選択します。
2. AWS アカウント ページの [組織構造] には、組織のルートと、その下にあるアカウントが階層内で表示されます。管理アカウントのチェックボックスをオンにし、[ユーザーまたはグループを割り当て] を選択します。
3. [ユーザーとグループを割り当てる] のワークフローが表示されます。これは、3 つのステップから構成されています。

   a. [ステップ 1: ユーザーとグループの選択] では、管理者の職務を実行するユーザーを選択します。次いで、[次へ] を選択します。

   b. [ステップ 2: アクセス許可セットの選択] では、[許可セットを作成] を選択します。新しいタブが開き、アクセス許可セットを作成するための 3 つのサブステップが順を追って表示されます。

      i. [ステップ 1: 許可セットタイプを選択] では、以下を完了します。

         - [許可セットのタイプ] で、[事前定義された許可セット] を選択します。
         - 事前定義されたアクセス許可セット のポリシーで、 を選択しますAdministratorAccess。

         [次へ] をクリックします。

      ii. [ステップ 2: 許可セットの詳細を指定] では、デフォルト設定のままで、[次へ] を選択します。

         デフォルト設定では、セッション時間を 1 時間に設定した という名前*AdministratorAccess*のアクセス許可セットが作成されます。

      iii. ステップ 3: を確認して作成する で、アクセス許可セットタイプが AWS 管理ポリシーを使用していることを確認しますAdministratorAccess。[作成] を選択します。[アクセス許可セット] ページに、アクセス許可セットが作成されたことを知らせる通知が表示されます。この時点で、ウェブブラウザでこのタブを閉じてもかまいません。

      iv. [ユーザーとグループを割り当てる] ブラウザタブでは、[ステップ 2: 許可セットを選択] でアクセス許可セットの作成ワークフローを開始した状態のままになっています。

v. [アクセス許可セット] 領域で、[更新] ボタンを選択します。作成したAdministratorAccessアクセス許可セットがリストに表示されます。そのアクセス許可セットのチェックボックスを選択したら、[次へ] を選択します。

c. [ステップ 3: 確認と送信] では、選択したユーザーとアクセス許可セットを確認し、[送信] を選択します。

ページが更新され、 AWS アカウント が設定されているというメッセージが表示されます。プロセスが完了するまで待ちます。

AWS アカウント ページに戻ります。が再プロビジョニングされ、更新されたアクセス許可セットが適用され AWS アカウント たことを通知する通知メッセージ。ユーザーがサインインすると、AdministratorAccessロールを選択するオプションがあります。

> **Note**
>
> からの SCIM 自動同期は、ユーザーのプロビジョニングGoogle Workspaceのみをサポートします。現時点では、グループの自動プロビジョニングはサポートされていません。 AWS Management Consoleを使用して Google Workspace ユーザーのグループを作成することはできません。ユーザーをプロビジョニングした後、AWS CLI Identity Store の create-group コマンドまたは IAM API を使用してグループを作成できますCreateGroup。

ステップ 7: Google Workspace: Google WorkspaceユーザーがAWS リソースにアクセスできることを確認する

1. テストユーザーアカウントGoogleを使用して にサインインします。にユーザーを追加する方法についてはGoogle Workspace、「Google Workspaceのドキュメント」を参照してください。
2. Google apps ランチャー (ワッフル) アイコンを選択します。
3. カスタム Google Workspace アプリが置かれているアプリケーションリストの下部にスクロールします。[Amazon Web Services] と [AWS アクセスポータル] の 2 つのアプリが表示されます。
4. AWS アクセスポータルアプリを選択します。ポータルにサインインすると、 AWS アカウント アイコンが表示されます。そのアイコンを展開すると、 AWS アカウント ユーザーがアクセスできる のリストが表示されます。このチュートリアルでは 1 つのアカウントしか使用していなかったため、アイコンを展開しても 1 つのアカウントしか表示されません。

> **Note**
>
> Amazon Web Services アプリを選択すると、SAML エラーが表示されます。このアプリは IAM ユーザーとしてプロビジョニングされた Google Workspace ユーザー用で、このチュートリアルでは IAM アイデンティティセンターのユーザーとして Google Workspace ユーザーをプロビジョニングします。

5. アカウントを選択すると、そのユーザーが利用可能なアクセス許可セットが表示されます。このチュートリアルでは、アクセスAdministratorAccess許可セットを作成しました。
6. アクセス許可セットの横には、その許可セットで利用できるアクセスの種類を示すリンクがあります。アクセス許可セットを作成したときに、管理コンソールとプログラムによるアクセスの両方を有効にするように指定したので、これら 2 つのオプションが表示されます。[管理コンソール] を選択して AWS Management Consoleを開きます。
7. ユーザーはコンソールにサインインしています。

(オプション) アクセスコントロールの属性を渡す

IAM Identity Center の アクセスコントロールの属性 機能をオプションで使用して、Name 属性を `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` に設定した `Attribute` 要素を渡すことができます。この要素を使用すると、SAML アサーションでセッションタグとして属性を渡すことができます。セッションタグの詳細については、「IAM ユーザーガイド」の「 AWS STSでのタグ付けの規則 」 を参照してください。

属性をセッションタグとして渡すには、タグの値を指定する `AttributeValue` 要素を含めます。例えば、タグのキーバリューのペア `CostCenter = blue` を渡すには、次のような属性を使用します。

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

複数の属性を追加する必要がある場合は、各タグに個別の `Attribute` 要素を含めます。

次のステップ

Google Workspace を ID プロバイダーとして設定し、IAM アイデンティティセンターにユーザーをプロビジョニングしたので、次のことが可能になります。

- AWS CLI Identity Store の create-group コマンドまたは IAM API を使用してCreateGroup、ユーザーのグループを作成します。

  グループは、 AWS アカウント およびアプリケーションへのアクセスを割り当てるときに便利です。各ユーザーを個別に割り当てるのではなく、グループに権限を与えます。その後、グループにユーザーを追加したり削除したりすると、そのユーザーはグループに割り当てられたアカウントやアプリケーションへのアクセス権を動的に得たり、失ったりします。
- 職務に基づいてアクセス許可を設定します。「アクセス許可セットの作成」を参照してください。

  アクセス権限セットは、ユーザーおよびグループが持つこの AWS アカウントアカウントに対するアクセスのレベルを定義します。権限セットは IAM Identity Center に保存され、1 つまたは複数の AWS アカウントにプロビジョニングできます。複数のアクセス権限セットを 1 人のユーザーに割り当てることができます。

> **Note**
>
> IAM Identity Center の管理者として、古い IdP 証明書を新しい証明書に置き換える必要がある場合があります。例えば、IdP 証明書の有効期限が近づいている場合は、証明書を交換する必要があります。古い証明書を新しい証明書に置き換えるプロセスは、証明書のローテーションと呼ばれています。Google Workspace については、SAML 証明書の管理方法を必ず確認してください。

IAM アイデンティティセンターを使用して JumpCloud ディレクトリプラットフォームに接続する

IAM Identity Center は、JumpCloud ディレクトリプラットフォームから IAM Identity Center へのユーザー情報の自動プロビジョニング (同期) をサポートします。このプロビジョニングでは、クロスドメインアイデンティティ管理システム (SCIM) v2.0 プロトコルを使用します。この接続を JumpCloud で設定するには、IAM Identity Center SCIM エンドポイントとアクセストークンを使用します。SCIM 同期を設定すると、JumpCloud のユーザー属性と IAM Identity Center の名前付き属性

のマッピングが作成されます。これにより、IAM Identity Center と JumpCloud の間で、期待される属性が一致します。

このガイドは、2021 年 6 月時点の JumpCloud に基づきます。新しいバージョンでは、手順が異なる場合があります。このガイドには、SAML によるユーザー認証の設定に関するいくつかの注意事項が記載されています。

次のステップでは、SCIM プロトコルを使用して、JumpCloud から IAM Identity Center へのユーザーとグループの自動プロビジョニングを有効にする方法を説明します。

> **Note**
>
> SCIM のデプロイを開始する前に、まず 自動プロビジョニングを使用する際の注意事項 を確認することをお勧めします。そして、次のセクションで残りの注意事項を確認します。

トピック

前提条件

開始する前に、以下の準備が必要です。

- JumpCloud のサブスクリプションまたは無料トライアル。無料トライアルにサインアップするには、JumpCloud にアクセスしてください。
- IAM Identity Center 対応アカウント (無料)。詳細については、「IAM Identity Center の有効化」を参照してください。
- 「JumpCloudIAM ID Centerのドキュメント」で説明されている、JumpCloud アカウントから IAM アイデンティティセンターへの SAML 接続。

- IAM Identity Center コネクターを、AWS アカウントへのアクセスを許可するグループに関連付けます。

SCIM に関する注意事項

IAM Identity Center に JumpCloud のフェデレーションを使用する場合の注意事項を以下に示します。

- JumpCloud の AWS シングルサインオンコネクターに関連するグループのみが SCIM を介して同期されます。
- 同期できる電話番号属性は 1 つだけです。デフォルトは「仕事用の電話」です。
- JumpCloud ディレクトリのユーザーは、SCIM 経由で IAM Identity Center に同期されるように姓名が設定されている必要があります。
- ユーザーが IAM Identity Center で無効化されていても、JumpCloud で有効化されていれば、属性は引き続き同期されます。
- コネクターの [Enable management of User Groups and Group membership] (ユーザーグループおよびグループメンバーシップの管理を有効にする) のチェックを外すことで、ユーザー情報だけの SCIM 同期を有効にすることができます。
- IAM Identity Center ディレクトリに同じユーザーネームと E メールアドレスを持つ既存のユーザーがいる場合、そのユーザーは上書きされ、JumpCloud から SCIM を介して同期されます。

ステップ 1: IAM Identity Center でプロビジョニングを有効にする

この最初のステップでは、IAM Identity Center コンソールを使用して、自動プロビジョニングを有効にします。

IAM Identity Center で自動プロビジョニングを有効にするには

1. 前提条件が整ったら、IAM Identity Center コンソールを開きます。
2. 左側のナビゲーションペインの [Settings] (設定) を選択します。
3. [設定] ページで、[自動プロビジョニング] 情報ボックスを探し、[有効化] を選択します。これにより、すぐに IAM Identity Center の自動プロビジョニングが有効になり、必要なエンドポイントとアクセストークンの情報が表示されます。

4. [Inbound automatic provisioning] (インバウンド自動プロビジョニング) ダイアログボックスで、以下のオプションの値をそれぞれコピーします。これらは、後で IdP でプロビジョニングを設定する際に貼り付ける必要があります。

   a. SCIM エンドポイント

   b. アクセストークン

5. [Close] (閉じる) を選択します。

IAM Identity Center でプロビジョニングを設定したので、JumpCloud IAM Identity Center を使用して残りのタスクを完了する必要があります。これらのステップについて、次の手順で説明します。

ステップ 2: JumpCloud でプロビジョニングを設定する

JumpCloud IAM ID センターコネクタで以下の手順を実行して、IAM ID センターによるプロビジョニングを有効にします。この手順では、JumpCloud IAM Identity Center が既に JumpCloud 管理者ポータルとグループに追加されていることを前提としています。まだ実行していない場合は、「前提条件」を参照してから、この手順を実行して SCIM プロビジョニングを設定してください。

JumpCloud でプロビジョニングを設定するには

1. JumpCloud 用 SAML 設定の一部としてインストールした JumpCloud IAM Identity Center コネクタを開きます([ユーザー認証] > [IAM Identity Center])。前提条件 を参照してください。
2. 「 IAM ID センター」コネクタを選択し、3 つ目のタブ「ID 管理」を選択します。
3. グループを SCIM 同期させたい場合は、[Enable management of User Groups and Group membership in this application] (このアプリケーションでのユーザーグループとグループメンバーシップの管理を有効にする) にチェックを入れます。
4. [Configure] (構成) をクリックします。
5. 前の手順で、IAM Identity Center から [SCIM エンドポイント] の値をコピーしました。その値を JumpCloud IAM Identity Center コネクターの [ベース URL] フィールドに貼り付けます。URL の末尾にあるスラッシュを削除してください。
6. 前の手順で、IAM Identity Center の [アクセストークン] の値をコピーしました。その値を JumpCloud IAM Identity Center コネクターの [トークンキー] フィールドに貼り付けます。
7. [Activate] (有効化) をクリックすると、設定が適用されます。
8. [Single Sign-On] (Single Sign-On) の横にある緑色のインジケータが有効になっていることを確認してください。

9. 4 つ目のタブ [ユーザーグループ] に移動し、SCIM でプロビジョニングしたいグループにチェックを入れます。
10. 完了したら、下部の [Save] (保存) をクリックします。
11. ユーザーが IAM Identity Center に正常に同期されたことを確認するには、IAM Identity Center コンソールに戻り、[ユーザー] を選択します。JumpCloud から同期されたユーザーは、[ユーザー] ページに表示されます。これらのユーザーは、IAM Identity Center でアカウントに割り当てられるようになりました。

(オプション) ステップ 3: IAM Identity Center でのアクセスコントロールのために JumpCloud でユーザー属性を設定する

これは、AWS リソースへのアクセスを管理するために IAM Identity Center の属性設定を選択した場合の JumpCloud のオプション手順です。JumpCloud で定義した属性は、SAML アサーションで IAM Identity Center に渡されます。その後、IAM Identity Center でアクセス権限セットを作成し、JumpCloud から渡された属性に基づいてアクセスを管理します。

この手順を始める前に、最初に [Attributes for access control] (アクセスコントロールのための属性) 機能を有効にしておく必要があります。これを行う方法については、「Enable and configure attributes for access control」(アクセスコントロールの属性を有効にし、設定する) を参照してください。

IAM Identity Center でのアクセスコントロールに使用される JumpCloud の属性の有効化と設定

1. JumpCloud 用 SAML 設定の一部としてインストールした JumpCloud IAM Identity Center コネクタを開きます([ユーザー認証] > [IAM Identity Center])。
2. IAM Identity Center コネクターを選択します。次に、2 つ目のタブ [IAM Identity Center] を選択します。
3. このタブの下部には、[ユーザー属性マッピング] があり、[A新規属性の追加] を選択して、以下の操作を行います。これらの手順は、IAM Identity Center でのアクセスコントロールに使用するために追加する各属性に行う必要があります。

    a. [サービス提供属性] フィールドには `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`AttributeName`**`.` を入力し、**`AttributeName`** は IAM Identity Center で想定している属性名に置き換えます。例えば、「`https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Email`**」と入力します。

b. [JumpCloud 属性名] フィールドで、JumpCloud ディレクトリからユーザー属性を選択します。例えば、E メール (仕事用)などです。

4. [保存] を選択します。

(オプション) アクセスコントロールの属性を渡す

IAM Identity Center の アクセスコントロールの属性 機能をオプションで使用して、Name 属性を `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` に設定した `Attribute` 要素を渡すことができます。この要素を使用すると、SAML アサーションでセッションタグとして属性を渡すことができます。セッションタグの詳細については、「IAM ユーザーガイド」の「AWS STS でのタグ付けの規則 」 を参照してください。

属性をセッションタグとして渡すには、タグの値を指定する `AttributeValue` 要素を含めます。例えば、タグのキーバリューのペア `CostCenter = blue` を渡すには、次のような属性を使用します。

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

複数の属性を追加する必要がある場合は、各タグに個別の `Attribute` 要素を含めます。

Microsoft Entra ID および IAM アイデンティティセンターによる SAML と SCIM の設定

AWS IAM Identity Center は、Security Assertion Markup Language (SAML) 2.0 との統合および、クロスドメイン ID 管理システム (SCIM) 2.0 プロトコルによる Microsoft Entra ID (旧称 Azure Active Directory または Azure AD) から IAM アイデンティティセンターへのユーザーとグループの情報の自動プロビジョニング (同期) をサポートしています。

目的

このチュートリアルでは、テストラボをセットアップし、Microsoft Entra ID と IAM アイデンティティセンター間の SAML 接続と SCIM プロビジョニングを設定します。最初の準備ステップでは、

両方向の SAML 接続をテストするのに使用する Microsoft Entra ID と IAM アイデンティティセンターの両方にテストユーザー (Nikki Wolf) を作成します。後で SCIM の手順の一環として、別のテストユーザー (Richard Roe) を作成して、Microsoft Entra ID の新しい属性が想定どおりに IAM アイデンティティセンターと同期されていることを確認します。

前提条件

このチュートリアルを開始する前に、まず以下を設定する必要があります。

- Microsoft Entra ID テナント。詳細については、マイクロソフトのウェブサイトの「Quickstart: Set up a tenant」(クイックスタート:テナントを設定する) を参照してください。
- AWS IAM Identity Center が有効なアカウント。詳細については、「AWS IAM Identity Centerユーザーガイド」の「 IAM アイデンティティセンターを有効にする」を参照してください。

ステップ 1: Microsoft テナントを準備する

このステップでは、AWS IAM Identity Center エンタープライズアプリケーションをインストールして構成し、新しく作成した Microsoft Entra ID テストユーザーにアクセス権を割り当てる方法について説明します。

Step 1.1 >

ステップ 1.1: Microsoft Entra ID で AWS IAM Identity Center エンタープライズアプリケーションを設定する

この手順では、AWS IAM Identity Center エンタープライズアプリケーションを Microsoft Entra ID にインストールします。このアプリケーションは、後で AWS との SAML 接続を設定する際に必要になります。

1. クラウドアプリケーション管理者以上の権限で、Microsoft Entra 管理センターにサインインします。
2. [ID] > [アプリケーション] > [エンタープライズアプリケーション] に移動し、[新しいアプリケーション] を選択します。
3. [Microsoft Entra ギャラリーの参照] ページで、検索ボックスに **`AWS IAM Identity Center`** を入力します。
4. 結果領域から AWS IAM Identity Center を選択します。
5. [Create] (作成) を選択します。

Step 1.2 >

ステップ 1.2: Microsoft Entra ID でテストユーザーを作成する

Nikki Wolf は、この手順で作成する Microsoft Entra ID テストユーザーの名前です。

1. Microsoft Entra 管理センターコンソールで、[ID] > [ユーザー] > [すべてのユーザー] に移動します。
2. [新しいユーザー] を選択し、画面上部の [新しいユーザーの作成] を選択します。
3. [ユーザープリンシパル名] に **NikkiWolf** と入力し、目的のドメインと拡張子を選択します。例えば、NikkiWolf@*example.org* と入力します。
4. [表示名] に **NikkiWolf** と入力します。
5. [パスワード] に、強力なパスワードを入力するか、目のアイコンを選択して自動生成されたパスワードを表示し、表示された値をコピーするか書き留めてください。
6. [プロパティ] を選択し、[名] に **Nikki** と入力します。[姓] に、**Wolf** と入力します。
7. [レビューと作成] を選択したら、[作成] を選択します。

Step 1.3

ステップ 1.3: Nikki に AWS IAM Identity Center へのアクセス権を割り当てる前に、Nikki のエクスペリエンスをテストする

この手順では、Nikki が Microsoft マイアカウントポータルに正常にサインインできることを確認します。

1. 同じブラウザで新しいタブを開き、マイアカウントポータルのサインインページに移動して、Nikki の完全なメールアドレスを入力します。例えば、NikkiWolf@*example.org* と入力します。
2. プロンプトが表示されたら、Nikki のパスワードを入力し、[サインイン] を選択します。これが自動生成されたパスワードの場合は、パスワードを変更するように求められます。
3. [アクションが必要] ページで [後で確認する] を選択すると、追加のセキュリティメソッドの入力を求めるプロンプトは表示されなくなります。
4. [マイアカウント] ページの左側のナビゲーションで、[マイアプリ] を選択します。現時点では、アドイン以外のアプリが表示されていないことに注意してください。後のステップでここに表示される AWS IAM Identity Center アプリを追加します。

Step 1.4

ステップ 1.4: Microsoft Entra ID で Nikki に権限を割り当てる

Nikki が [マイアカウントポータル] に正常にアクセスできることを確認したので、次の手順に従って Nikki のユーザーを AWS IAM Identity Center アプリに割り当てます。

1. Microsoft Entra 管理センターコンソールで、[ID] > [アプリケーション] > [エンタープライズアプリケーション] に移動し、リストから AWS IAM Identity Center を選択します。
2. 左側で [ユーザーとグループ] を選択します。
3. [Add user/group] (ユーザーとグループを追加) を選択します。グループを割り当てることができないというメッセージは無視してかまいません。このチュートリアルでは、割り当てにグループを使用しません。
4. [割り当てを追加] ページの [ユーザー] で、[何も選択されていません] を選択します。
5. [NikkiWolf] を選択し、次に [選択] を選択します。
6. [Add Assignment] (割り当てを追加) ページで、[Assign] (割り当て) を選択します。これで、AWS IAM Identity Center アプリに割り当てられたユーザーのリストに NikkiWolf が表示されるようになりました。

ステップ 2: AWS アカウントを準備する

このステップでは、IAM Identity Center を使用して (許可セットにより) アクセス許可を設定する方法、対応する Nikki Wolf ユーザを手動で作成する方法、および AWS のリソースを管理するために必要な権限をそのユーザに割り当てる方法について説明します。

Step 2.1 >

ステップ 2.1: IAM Identity Center で RegionalAdmin 許可セットを作成する

このアクセス許可セットを使用して、AWS Management Console内の [アカウント] ページからリージョンを管理するのに必要な AWS アカウント許可を Nikki に付与します。Nikki のアカウントのその他の情報を閲覧または管理するその他の権限は、デフォルトではすべて拒否されています。

1. IAM Identity Center コンソール を開きます。
2. [マルチアカウント権限] で、[権限セット] を選択します。
3. [Create permission set] (アクセス権限セットの作成) を選択します。
4. [許可セットタイプを選択] ページで [カスタム許可セット] を選択し、[次へ] を選択します。

5. [インラインポリシー] を選択して展開し、次の手順を使用してアクセス許可セットのポリシーを作成します。

   a. [新しいステートメントを追加] を選択してポリシーステートメントを作成します。

   b. [ステートメントを編集] で、リストから [アカウント] を選択し、次のチェックボックスを選択します。

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

   c. [リソースの追加] の横にある [追加] を選択します。

   d. [リソースを追加] ページの [リソースタイプ] で、[すべてのリソース] を選択し、[リソースを追加] を選択します。ポリシーが次のようになっていることを確認します。

```
{
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "account:ListRegions",
                "account:DisableRegion",
                "account:EnableRegion",
                "account:GetRegionOptStatus"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

6. [Next] (次へ) をクリックします。

7. [許可セットの詳細を指定] ページの [許可セット名] に **RegionalAdmin** と入力し、[次へ] を選択します。

8. [確認して作成] ページで、[作成] をクリックします。アクセス許可セットのリストに RegionalAdmin が表示されます。

Step 2.2 >

ステップ 2.2: IAM Identity Center で対応する NikkiWolf ユーザーを作成する

SAML プロトコルには IdP (Microsoft Entra ID) をクエリして IAM アイデンティティセンターで自動的にユーザーを作成するメカニズムがないため、次の手順に従って、Microsoft Entra ID の Nikki Wolfs ユーザーのコア属性をミラーリングするユーザーを IAM アイデンティティセンターに手動で作成します。

1. IAM Identity Center コンソールを開きます。
2. [ユーザー] を選択し、[ユーザーを追加] を選択して、次の情報を入力します。
   a. [ユーザー名] と [メールアドレス] の両方に、Microsoft Entra ID ユーザーを作成したときに使用したのと同じ **NikkiWolf@*yourcompanydomain.extension*** を入力します。例えば、NikkiWolf@*example.org* と入力します。
   b. [メールアドレスの確認] — 前のステップで使用したメールアドレスを再入力します。
   c. [名] — **Nikki** と入力します。
   d. [姓] — **Wolf** と入力します。
   e. [表示名] — **Nikki Wolf** と入力します。
3. [次へ] を 2 回選択後、[ユーザーの追加] を選択します。
4. [Close] を選択します。

Step 2.3

ステップ 2.3: IAM Identity Center で RegionalAdmin 許可セットに Nikki を割り当てる

ここで、Nikki がリージョンを管理する AWS アカウント を特定し、AWS アクセスポータルに正常にアクセスするために必要なアクセス許可を割り当てます。

1. IAM Identity Center コンソールを開きます。
2. [マルチアカウント権限] で、[AWS アカウント] を選択します。
3. Nikki にリージョンを管理するためのアクセス権を付与するアカウント名の横のチェックボックス (例えば、*Sandbox*) を選択し、[ユーザーとグループを割り当てる] を選択します。
4. [ユーザーとグループを割り当てる] ページで [ユーザー] タブを選択し、Nikki の横にあるボックスを探してオンにし、[次へ] を選択します。

ステップ 3: SAML 接続を設定してテストする

このステップでは、Microsoft Entra ID の AWS IAM Identity Center エンタープライズアプリケーションと IAM アイデンティティセンターの外部 IdP 設定を使用して SAML 接続を設定します。

Step 3.1 >

ステップ 3.1: IAM アイデンティティセンターから必要なサービスプロバイダーのメタデータを収集する

このステップでは、IAM アイデンティティセンターコンソール内から [ID ソースを変更] ウィザードを起動し、メタデータファイルと、次のステップで Microsoft Entra ID との接続を設定するときに入力する必要のある AWS 固有のサインイン URL を取得します。

1. [IAM Identity Center コンソール] で [設定] を選択します。
2. [設定] ページで [ID ソース] タブを選択し、[アクション] > [ID ソースを変更]を選択します。
3. [ID ソースを選択] ページで [外部 ID プロバイダー] を選択したら、[次へ] を選択します。
4. [外部 ID プロバイダーの設定] ページの [サービスプロバイダーメタデータ] で、[メタデータファイルをダウンロード] を選択してシステムにダウンロードします。
5. 同じセクションで、[AWS アクセスポータルのサインイン URL] 値を見つけてコピーします。この値は、次のステップで求められたときに入力します。
6. このページは開いたままにして、次のステップ (**`Step 3.2`**) に進み、Microsoft Entra ID の AWS IAM Identity Center エンタープライズアプリケーションを設定します。後でこのページに戻り、プロセスを完了します。

Step 3.2 >

ステップ 3.2: Microsoft Entra ID の AWS IAM Identity Center エンタープライズアプリケーションを設定する

この手順では、前のステップで取得したメタデータファイルの値とサインオン URL を使用して、Microsoft 側の SAML 接続の半分を確立します。

1. Microsoft Entra 管理センターコンソールで、[ID] > [アプリケーション] > [エンタープライズアプリケーション] に移動し、[AWS IAM Identity Center] を選択します。
2. 左側で [シングルサインオン] を選択します。

3. [Single Sign-On with SAML のセットアップ] ページで、[メタデータファイルのアップロード] を選択し、フォルダアイコンを選択し、前のステップでダウンロードしたサービスプロバイダーのメタデータファイルを選択して、[追加] を選択します。
4. [基本的な SAML 設定] ページで、[識別子] と [返信 URL] の値の両方が、`https://<REGION>.signin.aws.amazon.com/platform/saml/` で始まる AWS のエンドポイントを指していることを確認します。
5. [サインオン URL (オプション)] に、前のステップでコピーした AWS アクセスポータルのサインイン URL の値 (**Step 3.1**) を貼り付け、[保存] を選択したら、[X] を選択してウィンドウを閉じます。
6. AWS IAM Identity Center でシングルサインオンをテストするよう求められたら、[いいえ、後でテストします] を選択します。この検証は、後のステップで行います。
7. [SAML によるシングルサインオンの設定] ページの [SAML 証明書] セクションで、[フェデレーションメタデータ XML] の横にある [ダウンロード] を選択し、メタデータファイルをシステムに保存します。次のステップでプロンプトが表示されたら、このファイルをアップロードする必要があります。

Step 3.3 >

ステップ 3.3: AWS IAM Identity Center で Microsoft Entra ID の外部 IdP を設定する

ここで、IAM アイデンティティセンターコンソールの [ID ソースを変更] ウィザードに戻り、AWS の SAML 接続の後半を完了します。

1. IAM アイデンティティセンターコンソールで、**Step 3.1** で開いたままにしたブラウザセッションに戻ります。
2. [外部 ID プロバイダーの設定] ページの [ID プロバイダーのメタデータ] セクションの [IdP SAML メタデータ] で、[ファイルを選択] ボタンを選択し、前のステップで Microsoft Entra ID からダウンロードした ID プロバイダーのメタデータファイルを選択して、[開く] を選択します。
3. [Next] (次へ) をクリックします。
4. 免責事項を読み、次に進む準備ができたら、**ACCEPT** と入力してください。
5. [ID ソースを変更] を選択して変更を適用します。

Step 3.4 >

ステップ 3.4: Nikki が AWS アクセスポータルにリダイレクトされることをテストする

この手順では、Nikki の認証情報を使用して Microsoft の [マイアカウントポータル] にサインインして SAML 接続をテストします。認証されたら、Nikki を AWS アクセスポータルにリダイレクトする AWS IAM Identity Center アプリケーションを選択します。

1. マイアカウントポータルのサインインページに移動し、Nikki の完全なメールアドレスを入力します。例えば、**NikkiWolf**@*example.org* と入力します。
2. プロンプトが表示されたら、Nikki のパスワードを入力し、[サインイン] を選択します。
3. [マイアカウント] ページの左側のナビゲーションで、[マイアプリ] を選択します。
4. [マイアプリ] ページで、AWS IAM Identity Center という名前のアプリを選択します。これにより、追加の認証を求めるプロンプトが表示されます。
5. Microsoft のサインインページで、NikkiWolf の認証情報を選択します。2 度目に認証を求められたら、NikkiWolf の認証情報をもう一度選択してください。これにより、AWS アクセスポータルに自動的にリダイレクトされます。

> **Tip**
>
> 正常にリダイレクトされない場合は、[**Step 3.2**] に入力した AWS アクセスポータルのサインイン URL の値がコピー元 **Step 3.1** の値と一致することを確認してください。

6. [AWSアカウント] のアイコン

が表示されていることを確認します。

> **Tip**
>
> ページが空で、[AWS アカウント] アイコンが表示されない場合は、Nikki が [RegionalAdmin] 許可セットに正常に割り当てられたことを確認します (**Step 2.3** をご覧ください)。

Step 3.5

ステップ 3.5: Nikki が AWS アカウント を管理するためのアクセスレベルをテストする

このステップでは、Nikki が AWS アカウント のリージョン設定を管理するためのアクセスレベルを確認します。Nikki には、[アカウント] ページからリージョンを管理するための十分な管理者権限のみを持つことが期待されています。

1. AWS アクセスポータルで、[AWS アカウント] アイコン

   を選択してアカウントのリストを展開します。アイコンを選択すると、アクセス許可セットを定義したアカウントに関連付けられているアカウント名、アカウント ID、メールアドレスが表示されます。
2. アクセス許可セットを適用したアカウント名 (*Sandbox* など) を選択します (**Step 2.3** をご覧ください)。これにより、Nikki が自分のアカウントを管理するために選択できるアクセス許可セットのリストが展開されます。
3. RegionalAdmin の横にある [管理コンソール] を選択し、RegionalAdmin 許可セットで定義したロールを引き継ぎます。これにより、AWS Management Consoleホームページにリダイレクトされます。
4. コンソールの右上で、アカウント名を選択してから [アカウント] を選択します。これにより、[アカウント] ページに移動します。このページの他のすべてのセクションには、これらの設定を表示または変更するのに必要なアクセス許可がないことを示すメッセージが表示されます。
5. [アカウント] ページで、 [AWS リージョン] までスクロールダウンします。テーブル内の使用可能なリージョンのチェックボックスをオンにします。Nikki には、自分のアカウントのリージョンのリストを意図したとおりに [有効化] または [無効化] するために必要なアクセス許可が付与されています。

> よくできました!
>
> ステップ 1 ~ 3 は、SAML 接続の実装とテストを正常に実行するのに役立ちました。チュートリアルを完了するには、ステップ 4 に進んで自動プロビジョニングを実装することをお勧めします。

ステップ 4: SCIM 同期を設定してテストする

このステップでは、SCIM v2.0 プロトコルを使用して Microsoft Entra ID から IAM アイデンティティセンターへのユーザー情報の自動プロビジョニング (同期) を設定します。この接続を Microsoft

Entra ID IAM Identity Center 用の SCIM エンドポイントと IAM Identity Center で自動作成されたベアラートークンを使用して設定します。

SCIM 同期を設定すると、Microsoft Entra ID のユーザー属性と IAM Identity Center の名前付き属性のマッピングが作成されます。これにより、IAM Identity Center と Microsoft Entra ID の間で、期待される属性が一致します。

次のステップでは、Microsoft Entra ID の IAM アイデンティティセンターアプリを使って、主に Microsoft Entra ID に設置されたユーザーの IAM アイデンティティセンターへの自動プロビジョニングを有効にする方法を説明します。

Step 4.1 >

ステップ 4.1: Microsoft Entra ID で 2 人目のテストユーザーを作成する

テスト用に、Microsoft Entra ID で新しいユーザー (Richard Roe) を作成します。後で SCIM 同期を設定したら、このユーザーとすべての関連属性が IAM アイデンティティセンターと正常に同期されたことをテストします。

1. Microsoft Entra 管理センターコンソールで、[ID] > [ユーザー] > [すべてのユーザー] に移動します。
2. [新しいユーザー] を選択し、画面上部の [新しいユーザーの作成] を選択します。
3. [ユーザープリンシパル名] に **RichRoe** と入力し、目的のドメインと拡張子を選択します。例えば、RichRoe@*example.org* と入力します。
4. [表示名] に **RichRoe** と入力します。
5. [パスワード] に、強力なパスワードを入力するか、目のアイコンを選択して自動生成されたパスワードを表示し、表示された値をコピーするか書き留めてください。
6. [プロパティ] を選択し、以下の値を指定します。
   - [名] - **Richard** と入力します。
   - [姓] - **Roe** と入力します。
   - [役職名] - **Marketing Lead** と入力します。
   - [部門] - **Sales** と入力します。
   - [従業員 ID] - **12345** と入力します。
7. [レビューと作成] を選択したら、[作成] を選択します。

Step 4.2 >

ステップ 4.2: IAM アイデンティティセンターで自動プロビジョニングを有効にする

この手順では、IAM アイデンティティセンターコンソールを使用して、ユーザーとグループの Microsoft Entra ID から IAM アイデンティティセンターへの自動プロビジョニングを有効にします。

1. [IAM アイデンティティセンターコンソール] で、左のナビゲーションペインの [設定] を選択します。
2. [設定] ページの [ID ソース] タブで、[プロビジョニング方法] が [手動] に設定されていることに注目してください。
3. [自動プロビジョニング] 情報ボックスを見つけ、[有効にする] を選択します。これにより、すぐに IAM Identity Center の自動プロビジョニングが有効になり、必要なエンドポイントとアクセストークンの情報が表示されます。
4. [Inbound automatic provisioning] (インバウンド自動プロビジョニング) ダイアログボックスで、以下のオプションの値をそれぞれコピーします。これらは、次のステップで Microsoft Entra ID でプロビジョニングを設定する際に貼り付ける必要があります。

   a. [SCIM エンドポイント] - 例えば https://scim.*us-east-2*.amazonaws.com/*11111111111-2222-3333-4444-555555555555*/scim/v2/

   b. [アクセストークン] - [トークンを表示] を選択して値をコピーします。
5. [Close] (閉じる) を選択します。
6. [ID ソース] タブで、[プロビジョニング方法] が [SCIM] に設定されていることに注目してください。

Step 4.3 >

ステップ 4.3: Microsoft Entra ID の自動プロビジョニングを設定する

RichRoe テストユーザーが用意され、IAM アイデンティティセンターで SCIM を有効にしたので、Microsoft Entra ID で SCIM 同期設定の設定に進むことができます。

1. Microsoft Entra 管理センターコンソールで、[ID] > [アプリケーション] > [エンタープライズアプリケーション] に移動し、[AWS IAM Identity Center] を選択します。
2. [プロビジョニング] を選択し、[管理] で [プロビジョニング] をもう一度選択します。
3. [プロビジョニングモード] で [自動] を選択します。

4. [管理者認証情報] の [テナント URL] に、**Step 4.1** で先ほどコピーした [SCIM エンドポイント] URL 値を貼り付けます。[シークレットトークン] にアクセストークンの値を貼り付けます。
5. 接続のテストを選択します。テストした認証情報が正常に認証され、プロビジョニングが可能になったことを示すメッセージが表示されます。
6. [Save (保存)] を選択します。
7. [管理] で [ユーザーとグループ] を選択し、[ユーザー/グループの追加] を選択します。
8. [割り当てを追加] ページの [ユーザー] で、[何も選択されていません] を選択します。
9. [RichRoe] を選択後、[選択] を選択します。
10. [Add Assignment] (割り当てを追加) ページで、[Assign] (割り当て) を選択します。
11. [概要] を選択したら、[プロビジョニングの開始] を選択します。

Step 4.4

ステップ 4.4: 同期が行われたことを確認する

このセクションでは、Richard のユーザーが正常にプロビジョニングされ、すべての属性が IAM アイデンティティセンターに表示されていることを確認します。

1. IAM アイデンティティセンターコンソールで [ユーザー] をクリックします。
2. [ユーザー] ページに [RichRoe] ユーザーが表示されているはずです。[作成者] 列の値が [SCIM] に設定されていることに注意してください。
3. [RichRoe] を選択し、[プロファイル] で以下の属性が Microsoft Entra ID からコピーされていることを確認します。

   - [名] - **Richard**
   - [姓] - **Roe**
   - [部門] - **Sales**
   - 役職 - **Marketing Lead**
   - [従業員番号] - **12345**

   これで Richard のユーザーが IAM アイデンティティセンターで作成されたので、そのユーザーを任意のアクセス許可セットに割り当てて、AWS リソースに対する Richard のアクセスレベルを制御できます。例えば、以前に Nikki にリージョンを管理するためのアクセス許

可 (**Step 2.3** をご覧ください) を付与するために使用した **RegionalAdmin** 許可セットを [RichRoe] に割り当てた後、**Step 3.5** で RichRoe のアクセスレベルをテストできます。

> お疲れ様でした。
>
> Microsoft と AWS 間の SAML 接続が正常に設定され、自動プロビジョニングがすべてを同期させるために機能していることが確認できました。これで、学習した内容を応用して、本番環境をよりスムーズに設定できます。

Microsoft Entra ID で SCIM を運用環境で使用する場合の考慮事項

以下は、SCIM v2 プロトコルを使用して、本番環境内で IAM アイデンティティセンターを使用した自動プロビジョニングを実装するための計画に影響を与える場合がある Microsoft Entra ID に関する重要な考慮事項です。

> **Note**
>
> SCIM のデプロイを開始する前に、まず 自動プロビジョニングを使用する際の注意事項 を確認することをお勧めします。

アクセスコントロールの属性

アクセス制御の属性は、ID ソース内の誰が AWS リソースにアクセスできるかを決定するアクセス許可ポリシーで使用されます。Microsoft Entra ID のユーザーから属性を削除しても、IAM Identity Center の対応するユーザーからはその属性は削除されません。これは、Microsoft Entra ID の既知の制限事項です。ユーザーの属性が異なる (空でない) 値に変更された場合、その変更は IAM Identity Center に同期されます。

ネストされたグループ

Microsoft Entra ID ユーザープロビジョニングサービスは、ネストされたグループのユーザーを読み取ったりプロビジョニングしたりすることはできません。明示的に割り当てられたグループの直接のメンバであるユーザーのみが、読み取りとプロビジョニングを行うことができます。Microsoft Entra ID は、間接的に割り当てられたユーザまたはグループ (直接割り当てられたグループのメンバであるユーザまたはグループ) のグループ· メンバシップを再帰的に解凍することはありません。詳細については、「Microsoft Entra ID ドキュメント」の「割り当てベースのスコープ」を参照してください。

動的グループ

Microsoft Entra ID ユーザープロビジョニングサービスは、「動的グループ」のユーザーを読み取ってプロビジョニングできます。動的グループを使用する場合のユーザーとグループの構造と IAM Identity Center での表示方法を示す例については、以下を参照してください。これらのユーザーとグループは SCIM 経由で Microsoft Entra ID から IAM Identity Center にプロビジョニングされました。

たとえば、動的グループの Microsoft Entra ID 構造が以下のような場合：

1. メンバー ua1、ua2 を持つグループ A
2. メンバー ub1 を持つグループ B
3. メンバー uc1 を持つグループ C
4. グループ K (グループ A、B、C のメンバーを含むルールを持つ)
5. グループ L (グループ B と C のメンバーを含むルールを持つ)

ユーザとグループ情報が Microsoft Entra ID から SCIM を介して IAM Identity Center にプロビジョニングされた後、構造は以下のようになります。

1. メンバー ua1、ua2 を持つグループ A
2. メンバー ub1 を持つグループ B
3. メンバー uc1 を持つグループ C
4. メンバー ua1、ua2、ub1、uc1 を含むグループ K
5. メンバー ub1、uc1 を持つグループ L

動的グループを使用して自動プロビジョニングを設定する場合、次の考慮事項に留意してください。

- 動的グループにはネストされたグループを含めることができます。ただし、Microsoft Entra ID プロビジョニングサービスはネストされたグループをフラット化しません。たとえば、Microsoft Entra ID 動的グループの構造が以下のような場合：
  - グループ A はグループ B の親です。
  - グループ A には ua1 がメンバーとしています。
  - グループ B には ub1 がメンバーとしています。

グループ A を含む動的グループには、グループ A の直接のメンバー (つまり ua1) のみが含まれます。グループ B のメンバーは再帰的に含まれません。

- 動的グループには他の動的グループを含めることはできません。詳細については、Microsoft Entra ID ドキュメントの「プレビューに関する制限」を参照してください。

Microsoft Entra ID に関する SCIM の問題のトラブルシューティング

Microsoft Entra ID ユーザーが IAM アイデンティティセンターと同期しないという問題が発生している場合は、IAM アイデンティティセンターに新しいユーザーを追加する際に IAM アイデンティティセンターがフラグを立てた構文の問題が原因である可能性があります。これは、`'Export'` などの失敗したイベントに関する Microsoft Entra ID 監査ログで確認できます。このイベントの Status Reason (ステータス理由) には、次のように記述されます。

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

また、失敗したイベントの AWS CloudTrail を確認することもできます。これは、CloudTrail の Event History (イベントの履歴) コンソールで以下のフィルターを使って検索できます。

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

CloudTrail イベントのエラーには以下のように記載されます。

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

最終的に、この例外は、Microsoft Entra ID から渡された値の中に予想よりも多い値が含まれていたことを示しています。ここでの解決策は、Microsoft Entra ID のユーザー属性を調べ、重複した値がないことを確認することです。重複した値の一般的な例の一つは、携帯電話、仕事、FAX などの連絡先に複数の値が存在することです。別々の値ではありますが、これらはすべて 1 つの親属性 phoneNumbers として IAM Identity Center に渡されます。

一般的な SCIM のトラブルシューティングについては、「IAM Identity Center の問題のトラブルシューティング」をご覧ください。

ステップ 5: (オプション) ABAC を設定する

SAML と SCIM を正常に設定したので、属性ベースのアクセス制御 (ABAC) を任意で設定することができます。ABAC は、属性に基づいて権限を定義する認証戦略です。

Microsoft Entra ID では、次の 2 つの方法のいずれかを使用して、IAM アイデンティティセンターで使用するために ABAC を構成できます。

Method 1

方法 1: IAM アイデンティティセンターでのアクセス制御用に Microsoft Entra ID でユーザー属性を設定する

以下の手順では、AWS リソースへのアクセスを管理するために IAM アイデンティティセンターが Microsoft Entra ID のどの属性を使用すべきかを決定します。定義されると、Microsoft Entra ID は SAML アサーションを通じてこれらの属性を IAM Identity Center に送信します。その後、IAM Identity Center で アクセス権限セットを作成します。 を行い、Microsoft Entra ID から渡された属性に基づいてアクセスを管理する必要があります。

この手順を始める前に、まず アクセスコントロールの属性 機能を有効にしておく必要があります。これを行う方法については、「アクセスコントロールのための属性の有効化と設定」を参照してください。

1. Microsoft Entra 管理センターコンソールで、[ID] > [アプリケーション] > [エンタープライズアプリケーション] に移動し、[AWS IAM Identity Center] を選択します。
2. [Single Sign-On] (Single Sign-On) を選択します。
3. [属性とクレーム] セクションで、[編集] を選択します。
4. [属性とクレーム] ページで、以下を実行します。
    a. [Add new claim] (新しいクレームを追加する) を選択します。
    b. [Name] (名前) に `AccessControl:`*`AttributeName`* を入力します。*`AttributeName`* を IAM Identity Center で想定している属性名に置き換えます。例えば、`AccessControl:`**`Department`** です。
    c. Namespaceに **`https://aws.amazon.com/SAML/Attributes`**. と入力します。
    d. 出典 で、属性を選択します。
    e. [ソースの属性] で、ドロップダウンリストを使用して、[Microsoft Entra ID ユーザー属性] を選択します。例えば、`user.`**`department`** です。
5. SAML アサーションで IAM Identity Center に送信する必要のある各属性について、前のステップを繰り返します。
6. [Save (保存)] を選択します。

Method 2

方法 2: IAM アイデンティティセンターを使用して ABAC を構成する

この方法では、IAM Identity Center の アクセスコントロールの属性 機能を使って、Name 属性を `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` に設定した `Attribute` 要素を渡します。この要素を使用すると、SAML アサーションで属性をセッションタグとして渡すことができます。セッションタグの詳細については、「IAM ユーザーガイド」の「AWS STS でのタグ付けの規則 」 を参照してください。

属性をセッションタグとして渡すには、タグの値を指定する `AttributeValue` 要素を含めます。例えば、タグのキーバリューのペア `CostCenter = blue` を渡すには、次の属性を使用します。

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

複数の属性を追加する必要がある場合は、各タグに個別の `Attribute` 要素を含めます。

Okta および IAM アイデンティティセンターによる SAML と SCIM の設定

System for Cross-domain Identity Management (SCIM) v2.0 プロトコルを使用して、Okta からユーザーとグループの情報を IAM アイデンティティセンターに自動的にプロビジョニング (同期) できます。この接続を Okta で設定するには、IAM Identity Center 用の SCIM エンドポイントと、IAM Identity Center で自動的に作成されるベアラートークンを使用します。SCIM 同期を設定すると、Okta のユーザー属性と IAM Identity Center の名前付き属性のマッピングが作成されます。このマッピングは、IAM アイデンティティセンターと Okta の間で、期待されるユーザー属性を照合します。

Okta は、SCIM を介して IAM Identity Center に接続した場合、以下のプロビジョニング機能をサポートします。

- ユーザーの作成 — Okta で IAM Identity Center アプリケーションに割り当てられたユーザーは IAM ID センターでプロビジョニングされます。
- ユーザー属性の更新 — Okta で IAM Identity Center に割り当てられているユーザーの属性変更は、IAM Identity Center で更新されます。
- ユーザーの無効化 — Okta で IAM Identity Center から割り当てられていないユーザーは、IAM Identity Center では無効になります。
- グループプッシュ — Okta のグループ (およびそのメンバー) は、IAM Identity Center に同期されます。

> **Note**
>
> Okta と IAM Identity Center の両方で管理上のオーバーヘッドを最小限に抑えるために、個々のユーザーではなくグループを割り当てを行い、プッシュすることをお勧めします。

IAM アイデンティティセンターをまだ有効にしていない場合は、「の有効化 AWS IAM Identity Center」を参照してください。

目的

このチュートリアルでは、Okta IAM アイデンティティセンターとの SAML 接続をセットアップする手順を順を追って説明します。後で、SCIM を使用して Okta からのユーザーを同期します。このシナリオでは、Okta 内のすべてのユーザーとグループを管理します。ユーザーは Okta ポータルを通じてサインインします。すべてが正しく設定されていることを確認するには、設定ステップを完了すると、 Okta ユーザーとしてサインインし、 AWS リソースへのアクセスを確認します。

> **Note**
>
> Okta's IAM アイデンティティセンターアプリケーションがインストールされている Okta アカウント (無料トライアル) にサインアップできます。有料の Okta 製品の場合は、Okta のライセンスがライフサイクル管理やアウトバウンドプロビジョニングを可能にする同様の機能をサポートしているかどうかを確認する必要があるかもしれません。これらの機能は、Okta から IAM Identity Center に SCIM を設定する際に必要となる場合があります。

開始する前に

Okta と IAM Identity Center の間で SCIM プロビジョニングを設定する前に、まず を確認することをお勧めします自動プロビジョニングを使用する際の注意事項。

開始する前に、次について確認してください。

- すべての Okta ユーザーにおいて、[名]、[姓]、[ユーザー名]、[表示名] の値を指定する必要があります。
- 各 Okta ユーザーには、E メールアドレスや電話番号などのデータ属性ごとに 1 つの値のみが割り当てられます。複数の値を持つユーザーは同期に失敗します。属性に複数の値を持つユーザーがいる場合は、IAM アイデンティティセンターでユーザーをプロビジョニングする前に、重複する属性を削除してください。例えば、同期できる電話番号属性は 1 つだけです。デフォルトの電話番号属性は「勤務先の電話」なので、ユーザーの電話番号が自宅の電話でも携帯電話でも、「勤務先の電話」属性を使用してユーザーの電話番号を保存します。
- ユーザーの住所を更新する場合は、[streetAddress] (番地)、[city] (市町村)、[state] (都道府県)、[zipCode] (郵便番号)、[countryCode] (国番号) の値を指定する必要があります。同期する時に、これらの値のいずれかが Okta ユーザーに指定されていない場合、ユーザー (またはユーザーへの変更) はプロビジョニングされません。

> **Note**
>
> 資格とロール属性はサポートされていないため、IAM アイデンティティセンターと同期できません。
> 同じ Okta グループを割り当てとグループプッシュの両方に使用することは、現在サポートされていません。Okta と IAM アイデンティティセンターの間で一貫したグループメンバーシップを維持するためには、別のグループを作成し、IAM アイデンティティセンターにグループをプッシュするように設定する必要があります。

ステップ 1: Okta アカウントから SAML メタデータを取得する

1. Okta admin dashboard にログインして [アプリケーション] を展開し、[アプリケーション] を選択します。
2. [Applications] (アプリケーション) ページで、[Browse App Catalog] (アプリケーションカタログを参照) を選択します。

3. 検索ボックスに「」と入力し AWS IAM Identity Center、アプリを選択して IAM Identity Center アプリを追加します。
4. [サインオン] タブを選択します。
5. [SAML 署名証明書] で、[アクション] を選択し、[IdP メタデータの表示] を選択します。新しいブラウザタブが開き、XML ファイルのドキュメントツリーが表示されます。`<md:EntityDescriptor>` から `</md:EntityDescriptor>` まで XML をすべて選択し、テキストファイルにコピーします。
6. `metadata.xml` としてテキストファイルを保存します。

Okta admin dashboard は開いたままにしておき、後のステップでもそのコンソールを引き続き使用します。

ステップ 2: Okta を IAM アイデンティティセンターの ID ソースとして設定する

1. 管理者権限を持つユーザーとして IAM アイデンティティセンターコンソールを開きます。
2. 左側のナビゲーションペインの [Settings] (設定) を選択します。
3. [設定] ページで [アクション] タブを選択し、[ID ソースを変更] を選択します。
4. [ID ソースの選択] で [外部 ID プロバイダー] を選択し、[次へ] を選択します。
5. [外部 ID プロバイダーの設定] で、次の操作を行います。

   a. [サービスプロバイダーメタデータ] で、[メタデータファイルをダウンロード] を選択して、IAM アイデンティティセンターメタデータファイルをダウンロードし、システムに保存します。このチュートリアルの後半で、IAM アイデンティティセンターSAML メタデータファイルを Okta に提供します。

   簡単にアクセスできるように、以下の項目をテキストファイルにコピーします。

   - [IAM アイデンティティセンターアサーションコンシューマーサービス (ACS) URL]
   - [IAM アイデンティティセンター発行者 URL]

   これらの値は、このチュートリアルの後半で必要になります。

   b. ID プロバイダーメタデータ で、IdP SAML メタ で ファイルを選択 を選択し、前のステップで作成した`metadata.xml`ファイルを選択します。

   c. [次へ] をクリックします。
6. 免責事項を読み、次に進む準備ができたら、[ACCEPT] (許諾) を押してください。

7. [Change identity source] (ID ソースの変更) を選択します。

   AWS コンソールを開いたままにしておき、次のステップでそのコンソールを引き続き使用します。

8. Okta admin dashboard に戻り、 AWS IAM Identity Center アプリケーションの [サインオン] タブを選択し、[編集] をクリックします。

9. [詳細なサインオン設定] で、次のように入力します。

   - [ACS URL] には、[IAM アイデンティティセンターアサーションコンシューマーサービス (ACS) URL] にコピーした値を入力します。
   - [発行者 URL] には、[IAM アイデンティティセンターの発行者 URL] にコピーした値を入力します。
   - [アプリケーションのユーザー名形式] で、ドロップダウンメニューからいずれかのオプションを選択します。

     選択する値はユーザーごとに異なるようにしてください。このチュートリアルでは、[Okta ユーザー名] を選択します。

10. [保存] を選択します。

これで、IAM アイデンティティセンターでユーザーを Okta からプロビジョニングする準備が整いました。をOkta admin dashboard開いたままにして、次のステップのために IAM Identity Center コンソールに戻ります。

ステップ 3: Okta からユーザーをプロビジョニングするには

1. IAM アイデンティティセンターコンソールの [設定] ページで、[自動プロビジョニング] 情報ボックスを見つけて、[有効にする] を選択します。これにより、IAM アイデンティティセンターの自動プロビジョニングが有効になり、必要な SCIM エンドポイントとアクセストークンの情報が表示されます。

2. [インバウンド自動プロビジョニング] ダイアログボックスで、以下のオプションの値をそれぞれコピーします。

   - SCIM エンドポイント
   - アクセストークン

このチュートリアルの後半では、これらの値を入力して、 でプロビジョニングを設定します Okta。

3. [閉じる] を選びます。
4. Okta admin dashboard に戻り、IAM アイデンティティセンターアプリに移動します。
5. IAM Identity Center アプリページでプロビジョニングタブを選択し、設定 の左側のナビゲーションで統合 を選択します。
6. 編集 を選択し、API 統合を有効にする の横にあるチェックボックスを選択してプロビジョニングを有効にします。
7. このチュートリアルの先ほどコピーした IAM アイデンティティセンターの SCIM プロビジョニング値を使用して Okta を設定します。

   a. [ベース URL] フィールドに [SCIM エンドポイント] の値を入力します。URL の末尾にあるスラッシュを削除してください。

   b. [API トークン] フィールドに、[アクセストークン] の値を入力します。
8. [Test API Credentials] (API 認証情報をテストする) を選択して、入力された認証情報が有効であることを確認します。

   [AWS IAM Identity Center は正常に検証されました] というメッセージが表示されます。
9. [保存] を選択します。統合 が選択された状態で、 設定 エリアに移動します。
10. 「設定」で、「アプリケーションへ」を選択し、有効にするアプリへのプロビジョニング機能ごとに「有効化」チェックボックスを選択します。このチュートリアルでは、すべてのオプションを選択します。
11. [保存] を選択します。

これで、IAM アイデンティティセンターでユーザーを Okta から同期する準備が整いました。

ステップ 4: Okta から IAM アイデンティティセンターとユーザーを同期する

デフォルトでは、Okta IAM アイデンティティセンターアプリにはグループやユーザーは割り当てられていません。プロビジョニンググループは、グループのメンバーであるユーザーをプロビジョニングします。グループとユーザーを IAM アイデンティティセンターと同期するには、以下の手順を実行します。

1. Okta IAM Identity Center アプリページで、「割り当て」タブを選択します。IAM アイデンティティセンターアプリにはユーザーとグループの両方を割り当てることができます。

a. ユーザーを割り当てるには:

- [割り当て] ページで、[割り当てる] を選択し、[人に割り当てる] を選択します。
- IAM アイデンティティセンターアプリへのアクセスを付与する Okta ユーザーを選択します。[Assign] (割り当て)、[Save and Go Back] (保存して戻る)、[Done] (完了) の順に選択します。

これにより、IAM アイデンティティセンターへのユーザーのプロビジョニングプロセスが開始されます。

b. グループを割り当てるには:

- [割り当て] ページで、[割り当てる] を選択し、[グループに割り当てる] を選択します。
- IAM アイデンティティセンターアプリへのアクセスを付与する Okta グループを選択します。[Assign] (割り当て)、[Save and Go Back] (保存して戻る)、[Done] (完了) の順に選択します。

これにより、IAM Identity Center へのグループ内のユーザーのプロビジョニングプロセスが開始されます。

> **Note**
>
> グループに追加の属性がすべてのユーザーレコードに含まれていない場合は、その属性を指定する必要がある場合があります。グループに指定された属性は、個々の属性値よりも優先されます。

2. [Push Groups] (プッシュグループ) タブを選択します。IAM アイデンティティセンターアプリに割り当てたすべてのグループを含む Okta グループを選択します。[保存] を選択します。

   グループとそのメンバーが IAM アイデンティティセンターに正常にプッシュされると、グループのステータスが [アクティブ] に変わります。

3. [割り当て] タブに戻ります。
4. IAM アイデンティティセンターにプッシュしたグループのメンバーではないユーザーがいる場合は、以下の手順を使用してユーザーを個別に追加します。

   [Assignments] (割り当て) ページで、[Assign] (割り当て) を選択し、[Assign to People] (人に割り当てる) を選択します。

5. IAM アイデンティティセンターアプリへのアクセスを付与する Okta ユーザーを選択します。[Assign] (割り当て)、[Save and Go Back] (保存して戻る)、[Done] (完了) の順に選択します。

   これにより、IAM アイデンティティセンターへの個人ユーザーのプロビジョニングプロセスが開始されます。

   > **Note**
   >
   > のアプリケーションページから AWS IAM Identity Center 、ユーザーとグループをアプリケーションに割り当てることもできますOkta admin dashboard。これを行うには、[設定] アイコンを選択し、[ユーザーに割り当てる] または [グループに割り当てる] を選択し、ユーザーまたはグループを指定します。

6. IAM アイデンティティセンターコンソールに戻ります。左側のナビゲーションで [ユーザー] を選択すると、Okta ユーザーが入力したユーザーリストが表示されます。

> **お疲れ様でした。**
>
> Okta と の間の SAML 接続を正常にセットアップ AWS し、自動プロビジョニングが機能していることを検証しました。[IAM Identity Center] でこれらのユーザーをアカウントおよびアプリケーションに割り当てることができるようになりました。このチュートリアルでは、次のステップで、管理アカウントへの管理アクセス許可を付与して、ユーザーの 1 人を IAM アイデンティティセンター管理者として指定しましょう。

ステップ 5: Okta ユーザーにアカウントへのアクセス権を付与する

1. IAM アイデンティティセンターのナビゲーションペインの [マルチアカウントのアクセス許可] で、[AWS アカウント] を選択します。
2. AWS アカウント ページの [組織構造] には、組織のルートと、その下にあるアカウントが階層内で表示されます。管理アカウントのチェックボックスをオンにし、[ユーザーまたはグループを割り当て] を選択します。
3. [ユーザーとグループを割り当てる] のワークフローが表示されます。これは、3 つのステップから構成されています。

a. [ステップ 1: ユーザーとグループの選択] では、管理者の職務を実行するユーザーを選択します。次いで、[次へ] を選択します。

b. [ステップ 2: アクセス許可セットの選択] では、[許可セットを作成] を選択します。新しいタブが開き、アクセス許可セットを作成するための 3 つのサブステップが順を追って表示されます。

   i. [ステップ 1: 許可セットタイプを選択] では、以下を完了します。

      - [許可セットのタイプ] で、[事前定義された許可セット] を選択します。
      - 事前定義されたアクセス許可セット のポリシーで、 を選択しますAdministratorAccess。

      [次へ] をクリックします。

   ii. [ステップ 2: 許可セットの詳細を指定] では、デフォルト設定のままで、[次へ] を選択します。

      デフォルト設定では、セッション時間を 1 時間に設定した という名前*AdministratorAccess*のアクセス許可セットが作成されます。

   iii. ステップ 3: を確認して作成する で、アクセス許可セットタイプが AWS 管理ポリシーを使用していることを確認しますAdministratorAccess。[作成] を選択します。[アクセス許可セット] ページに、アクセス許可セットが作成されたことを知らせる通知が表示されます。この時点で、ウェブブラウザでこのタブを閉じてもかまいません。

   [ユーザーとグループを割り当てる] ブラウザタブでは、[ステップ 2: 許可セットを選択] でアクセス許可セットの作成ワークフローを開始した状態のままになっています。

   [アクセス許可セット] 領域で、[更新] ボタンを選択します。作成した*AdministratorAccess*アクセス許可セットがリストに表示されます。そのアクセス許可セットのチェックボックスを選択したら、[次へ] を選択します。

c. [ステップ 3: 確認と送信] では、選択したユーザーとアクセス許可セットを確認し、[送信] を選択します。

   ページが更新され、 AWS アカウント が設定されているというメッセージが表示されます。プロセスが完了するまで待ちます。

AWS アカウント ページに戻ります。が再プロビジョニングされ、更新されたアクセス許可セットが適用され AWS アカウント たことを通知する通知メッセージ。ユーザーがサインインすると、*AdministratorAccess*ロールを選択するオプションがあります。

> **Note**
>
> Okta からの SCIM 自動同期はユーザーのプロビジョニングのみをサポートし、グループは自動的にプロビジョニングされません。 AWS Management Consoleを使用して Okta ユーザーのグループを作成することはできません。ユーザーをプロビジョニングしたら、CLI または API 操作によってグループを作成できます。

ステップ 6: Oktaユーザーが AWS リソースにアクセスできることを確認する

1. テストユーザーアカウントを使用して Okta dashboard にサインインします。
2. [マイアプリ] で、AWS IAM Identity Center アイコンを選択します。
3. ポータルにサインインすると、 AWS アカウント アイコンが表示されます。そのアイコンを展開すると、 AWS アカウント ユーザーがアクセスできる のリストが表示されます。このチュートリアルでは 1 つのアカウントしか使用していなかったため、アイコンを展開しても 1 つのアカウントしか表示されません。
4. アカウントを選択すると、そのユーザーが利用可能なアクセス許可セットが表示されます。このチュートリアルでは、アクセスAdministratorAccess許可セットを作成しました。
5. アクセス許可セットの横には、その許可セットで利用できるアクセスの種類を示すリンクがあります。アクセス許可セットを作成したときに、管理コンソールとプログラムによるアクセスの両方を有効にするように指定したので、これら 2 つのオプションが表示されます。[管理コンソール] を選択して AWS Management Consoleを開きます。
6. ユーザーはコンソールにサインインしています。

(オプション) アクセスコントロールの属性を渡す

IAM Identity Center の アクセスコントロールの属性 機能をオプションで使用して、Name 属性を `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` に設定した `Attribute` 要素を渡すことができます。この要素を使用すると、SAML アサーションでセッションタグとして属性を渡すことができます。セッションタグの詳細については、「IAM ユーザーガイド」の「 AWS STSでのタグ付けの規則 」 を参照してください。

属性をセッションタグとして渡すには、タグの値を指定する `AttributeValue` 要素を含めます。例えば、タグのキーバリューのペア `CostCenter = blue` を渡すには、次のような属性を使用します。

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

複数の属性を追加する必要がある場合は、各タグに個別の `Attribute` 要素を含めます。

次のステップ

Okta を ID プロバイダーとして設定し、IAM アイデンティティセンターにユーザーをプロビジョニングしたので、次のことが可能になります。

- へのアクセスを許可するには AWS アカウント、「」を参照してくださいへのユーザーアクセスを割り当てる AWS アカウント。
- クラウドアプリケーションへのアクセスを許可し、「IAM Identity Center コンソールでアプリケーションへのユーザーアクセスを割り当てます。」を参照してください。
- 職務に基づいてアクセス許可を設定します。「アクセス許可セットの作成」を参照してください。

OneLogin と IAM アイデンティティセンター間の SCIM プロビジョニングのセットアップ

IAM Identity Center は、クロスドメインアイデンティティ管理システム (SCIM) v2.0 プロトコルを使用して、OneLogin から IAM Identity Center へのユーザーおよびグループ情報の自動プロビジョニング (同期化) をサポートしています。この接続を OneLogin で設定するには、IAM Identity Center 用の SCIM エンドポイントと IAM Identity Center で自動的に作成したベアラートークンを使用します。SCIM 同期を設定すると、OneLogin のユーザー属性と IAM Identity Center の名前付き属性のマッピングが作成されます。これにより、IAM Identity Center と OneLogin の間で、期待される属性が一致します。

次のステップでは、SCIM プロトコルを使用して、OneLogin から IAM Identity Center へのユーザーとグループの自動プロビジョニングを有効にする方法を説明します。

> **Note**
>
> SCIM のデプロイを開始する前に、まず 自動プロビジョニングを使用する際の注意事項 を確認することをお勧めします。

トピック

前提条件

開始する前に、以下の準備が必要です。

- OneLogin アカウント。既存のアカウントをお持ちでない場合は、OneLogin のウェブサイトから無料トライアルまたはデベロッパーアカウントを取得できるかもしれません。
- IAM Identity Center 対応アカウント (無料)。詳細については、「IAM Identity Center の有効化」を参照してください。
- OneLogin アカウントから IAM Identity Center への SAML 接続。詳細については、AWS パートナーネットワークブログの「OneLogin と AWS の間の有効化」 を参照してください。

ステップ 1: IAM Identity Center でプロビジョニングを有効にする

この最初のステップでは、IAM Identity Center コンソールを使用して、自動プロビジョニングを有効にします。

IAM Identity Center で自動プロビジョニングを有効にするには

1. 前提条件が整ったら、IAM Identity Center コンソールを開きます。
2. 左側のナビゲーションペインの [Settings] (設定) を選択します。

3. [設定] ページで、[自動プロビジョニング] 情報ボックスを探し、[有効化] を選択します。これにより、すぐに IAM Identity Center の自動プロビジョニングが有効になり、必要なエンドポイントとアクセストークンの情報が表示されます。
4. [Inbound automatic provisioning] (インバウンド自動プロビジョニング) ダイアログボックスで、以下のオプションの値をそれぞれコピーします。これらは、後で IdP でプロビジョニングを設定する際に貼り付ける必要があります。

   a. SCIM エンドポイント

   b. アクセストークン
5. [Close] (閉じる) を選択します。

IAM Identity Center コンソールでプロビジョニングを設定しています。あとは OneLogin 管理者コンソールのユーザーインターフェースに従い、以下の残りの手順を行う必要があります。

ステップ 2: OneLogin でプロビジョニングを設定する

OneLogin 管理コンソールで以下の手順を使用して、IAM Identity Center と IAM Identity Center アプリケーション間の統合を有効にします。この手順では、AWS の OneLogin シングルサインオンアプリケーションで SAML 認証が設定済みであることを前提としています。この SAML 接続をまだ作成していない場合は、先に進む前に SAML 接続を作成し、ここに戻って SCIM のプロビジョニングプロセスを完了してください。OneLogin での SAML の設定の詳細については、AWS パートナーネットワークブログの「Enabling Single Sign-On Between OneLogin and AWS」を参照してください。

OneLogin でプロビジョニングを設定するには

1. OneLogin にサインインして、[アプリケーション] > [アプリケーション] と進みます。
2. [アプリケーション] ページで、IAM Identity Center との SAML 接続を形成するために以前に作成したアプリケーションを検索します。それを選択して、左のナビゲーションバーから [Configuration] (構成) を選択します。
3. 前の手順で、IAM Identity Center から [SCIM エンドポイント] の値をコピーしました。その値を OneLogin の [ベース URL] フィールドに貼り付けます。URL の末尾にあるスラッシュを削除してください。また、前の手順で、IAM Identity Center の [アクセストークン] の値をコピーしました。その値を OneLogin の [SCIM ベアラートークン] フィールドに貼り付けます。
4. [API Connection] (API 接続) の隣にある [Enable] (有効化) をクリックし、[Save] (保存) をクリックして設定を完了します。
5. 左側のナビゲーションバーで、[Provisioning] (プロビジョニング) を選択します。

6. [Enable provisioning] (プロビジョニングの有効化)、[Create user] (ユーザーの作成)、[Delete user] (ユーザーの削除)、[Update user] (ユーザーの更新) の各チェックボックスを選択し、[Save] (保存) を選択します。
7. 左側のナビゲーションバーで [Users] (ユーザー) を選択します。
8. [More Actions] (その他のアクション) をクリックして、[Sync logins] (ログイン同期) を選択します。[Synchronizing users with AWS Single Sign-On を使用したユーザーの同期] というメッセージが表示されます。
9. もう一度 [More Actions] (その他のアクション) をクリックして、[Reapply entitlement mappings] (エンタイトルメントマッピングの再適用) を選択します。Mappings are being reapplied (マッピングが再適用されている) というメッセージが表示されます。
10. この時点で、プロビジョニングプロセスを開始する必要があります。これを確認するには、[Activity] (アクティビティ) > Events (イベント) をクリックして、進行状況をモニタリングします。プロビジョニングに成功したイベントやエラーがイベントストリームに表示されます。
11. ユーザーおよびグループが IAM Identity Center にすべて正常に同期されたことを確認するには、 IAM Identity Center コンソールに戻り、[ユーザー] を選択します。OneLogin から同期されたユーザーは、[ユーザー] ページに表示されます。また、同期したグループは [Groups] (グループ) ページで確認できます。
12. ユーザーの変更を IAM Identity Center に自動的に同期させるには、[プロビジョニング] ページに移動し、[この操作を実行する前に管理者の承認を要求する] セクションを見つけ、[ユーザーの作成]、[ユーザーの削除]、[ユーザーの更新] の選択を解除し、[保存] をクリックします。

(オプション) ステップ 3: IAM Identity Center でのアクセスコントロールのために OneLogin でユーザー属性を設定する

これは、AWS リソースへのアクセスを管理するために IAM Identity Center の属性設定を選択した場合の OneLogin のオプション手順です。OneLogin で定義した属性は、SAML アサーションで IAM Identity Center に渡されます。その後、IAM Identity Center でアクセス権限セットを作成し、OneLogin から渡された属性に基づいてアクセスを管理します。

この手順を始める前に、最初に アクセスコントロールの属性 機能を有効にしておく必要があります。これを行う方法については、「アクセスコントロールのための属性の有効化と設定」を参照してください。

IAM Identity Center でのアクセスコントロールに使用される OneLogin の属性の有効化と設定

1. OneLogin にサインインして、[アプリケーション] > [アプリケーション] と進みます。

2. [アプリケーション] ページで、IAM Identity Center との SAML 接続を形成するために以前に作成したアプリケーションを検索します。それを選択して、左のナビゲーションバーから [Parameters] (パラメータ) を選択します。
3. [必須パラメータ] セクションでは、IAM Identity Center で使用する各属性について以下のように設定します。

   a. + を選択します。

   b. [名前] フィールドには `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`AttributeName`** を入力し、**`AttributeName`** は IAM Identity Center で想定している属性名に置き換えます。例えば、「`https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Department`**」と入力します。

   c. [Flags] (フラグ) で、[Include in SAML assertion] (SAML アサーションに含める) の横のボックスをチェックして、[Save] (保存) を選択します。

   d. [値] フィールドでは、ドロップダウンリストを使って、OneLogin のユーザー属性を選択します。例えば、Department (部署) などです。
4. [保存] を選択します。

(オプション) アクセスコントロールの属性を渡す

IAM Identity Center の アクセスコントロールの属性 機能をオプションで使用して、`Name` 属性を `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`** に設定した `Attribute` 要素を渡すことができます。この要素を使用すると、SAML アサーションでセッションタグとして属性を渡すことができます。セッションタグの詳細については、「IAM ユーザーガイド」の「AWS STS でのタグ付けの規則 」 を参照してください。

属性をセッションタグとして渡すには、タグの値を指定する `AttributeValue` 要素を含めます。例えば、タグのキーバリューのペア `CostCenter = blue` を渡すには、次のような属性を使用します。

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

複数の属性を追加する必要がある場合は、各タグに個別の `Attribute` 要素を含めます。

トラブルシューティング

以下は、OneLogin で自動プロビジョニングで発生する問題のトラブルシューティングに役立ちます。

グループは IAM Identity Center にプロビジョニングされない

デフォルトでは、グループは OneLogin から IAM Identity Center にプロビジョニングできません。OneLogin で IAM Identity Center アプリケーションのグループプロビジョニングが有効になっていることを確認します。これを行うには、OneLogin 管理コンソールにサインインし、IAM Identity Center アプリケーションのプロパティ (IAM Identity Center アプリケーション > パラメータ > グループ) で、[ユーザープロビジョニングに含める] オプションが選択されている必要があります。SCIM のグループとして OneLogin のロールを同期させる方法を含め、OneLogin でグループを作成する方法の詳細については、「OneLogin のウェブサイト」 を参照してください。

すべての設定が正しいにもかかわらず、OneLogin から IAM Identity Center へ何も同期されない

上記の管理者承認に関する注意事項に加えて、多くの設定変更を有効にするためには、エンタイトルメントマッピングを再適用する必要があります。これは、[アプリケーション] > [アプリケーション] > [IAM Identity Center アプリケーション] > [その他のアクション] で確認できます。同期イベントを含む OneLogin のほとんどのアクションの詳細と口グは、[Activity] (アクティビティ) > [Events] (イベント) で確認できます。

OneLogin でグループを削除または無効にしたが、IAM Identity Center でまだ表示されている

OneLogin は現在、グループに対する SCIM DELETE オペレーションをサポートしていないため、グループは IAM Identity Center で存在し続けます。そのため、IAM Identity Center からグループを直接削除して、そのグループに対応する IAM Identity Center 内のアクセス権限が削除されるようにする必要があります。

OneLogin からグループを削除せずに IAM Identity Center でグループを削除したら、ユーザー/グループの同期問題が発生した

この問題を解決するには、まず、OneLogin に冗長なグループプロビジョニングルールや構成がないことを確認してください。例えば、アプリケーションに直接割り当てられたグループと、同じグループに発行するルールなどです。次に、IAM Identity Center 内の不必要なグループを削除します。最後に OneLogin でエンタイトルメントを リフレッシュして ([IAM Identity Center アプリケーション] > [プロビジョニング] > [エンタイトルメント])、エンタイトルメントマッピングを再度適用します ([IAM Identity Center アプリケーション] > [その他のアクション])。今後この問題を回避するには、ま

ず OneLogin でグループのプロビジョニングを停止するように変更し、その後 IAM Identity Center からグループを削除します。

IAM アイデンティティセンターで Ping Identity 製品を使用する

以下の Ping Identity 製品は、IAM Identity Center でテストされます。

トピック

PingFederate

IAM Identity Center は、Ping Identity (以下、Ping) の PingFederate 製品から IAM Identity Center へのユーザーおよびグループ情報の自動プロビジョニング (同期化) をサポートしています。このプロビジョニングでは、クロスドメインアイデンティティ管理システム (SCIM) v2.0 プロトコルを使用します。この接続を PingFederate で設定するには、IAM Identity Center SCIM エンドポイントとアクセストークンを使用します。SCIM 同期を設定すると、PingFederate のユーザー属性と IAM Identity Center の名前付き属性のマッピングが作成されます。これにより、IAM Identity Center と PingFederate の間で、期待される属性が一致します。

このガイドは、PingFederate バージョン 10.2 に基づいています。他のバージョンでは、手順が異なる場合があります。他のバージョンの Ping の IAM Identity Center へのプロビジョニングの設定方法の詳細については、PingFederate にお問い合わせください。

次のステップでは、SCIM プロトコルを使用して、PingFederate から IAM Identity Center へのユーザーとグループの自動プロビジョニングを有効にする方法を説明します。

> **Note**
>
> SCIM のデプロイを開始する前に、まず 自動プロビジョニングを使用する際の注意事項 を確認することをお勧めします。そして、次のセクションで残りの注意事項を確認します。

トピック

前提条件

開始する前に、以下の準備が必要です。

- 動作中の PingFederate サーバー。既存の PingFederate サーバーをお持ちでない場合は、Ping Identity のウェブサイトから無料トライアルまたはデベロッパーアカウントを取得できるかもしれません。無料トライアルには、ライセンスやソフトウェアのダウンロード、関連するドキュメントが含まれています。
- PingFederate サーバーにインストールされている PingFederate IAM Identity Center ソフトウェアのコピー。このソフトウェアの入手方法については、ing Identity ウェブサイトの「IAM Identity Center コネクター」を参照してください。
- IAM Identity Center 対応アカウント (無料)。詳細については、「IAM Identity Center の有効化」を参照してください。
- PingFederate インスタンスから IAM Identity Center への SAML 接続。この接続を設定する手順については、PingFederate のドキュメントを参照してください。つまり推奨される方法は、IAM Identity Center コネクターを使用して PingFederate で「ブラウザ SSO」を構成し、両端のメタデータの「ダウンロード」および「インポート」機能を使用して、PingFederate と IAM Identity Center の間で SAML メタデータを交換します。

追加の考慮事項

以下は、IAM Identity Center によるプロビジョニングの実装方法に影響を与える可能性がある PingFederate に関する重要な注意事項です。

- PingFederate で設定したデータストアのユーザーから属性 (電話番号など) を削除しても、IAM Identity Center に対応するユーザーからはその属性は削除されません。これは、PingFederate's のプロビジョナーの実装における既知の制限です。ユーザーの属性が異なる (空でない) 値に変更された場合、その変更は IAM Identity Center に同期されます。

ステップ 1: IAM Identity Center でプロビジョニングを有効にする

この最初のステップでは、IAM Identity Center コンソールを使用して、自動プロビジョニングを有効にします。

IAM Identity Center で自動プロビジョニングを有効にするには

1. 前提条件が整ったら、IAM Identity Center コンソールを開きます。
2. 左側のナビゲーションペインの [Settings] (設定) を選択します。
3. [設定] ページで、[自動プロビジョニング] 情報ボックスを探し、[有効化] を選択します。これにより、すぐに IAM Identity Center の自動プロビジョニングが有効になり、必要なエンドポイントとアクセストークンの情報が表示されます。
4. [Inbound automatic provisioning] (インバウンド自動プロビジョニング) ダイアログボックスで、以下のオプションの値をそれぞれコピーします。これらは、後で IdP でプロビジョニングを設定する際に貼り付ける必要があります。
   a. SCIM エンドポイント
   b. アクセストークン
5. [Close] (閉じる) を選択します。

IAM Identity Center コンソールでプロビジョニングを設定した後、PingFederate 管理コンソールを使用して残りのタスクを完了する必要があります。

ステップ 2: PingFederate でプロビジョニングを設定する

PingFederate 管理コンソールで以下の手順を使用して、IAM Identity Center と IAM Identity Center コネクター間の統合を有効にします。この手順では、IAM Identity Center コネクターソフトウェアが既にインストールされていることを前提としています。まだ実行していない場合は、「前提条件」を参照してから、この手順を実行して SCIM プロビジョニングを設定してください。

> **Important**
>
> PingFederate サーバーが以前にアウトバウンド SCIM プロビジョニング用に設定されていない場合は、プロビジョニングを有効にするために設定ファイルの変更が必要になることがあります。詳細については、Ping ドキュメントを参照してください。つまり、pingfederate-<version>/pingfederate/bin/run.properties ファイル内の `pf.provisioner.mode` 設定を `OFF` (デフォルト) 以外の値に変更して、現在稼働中のサーバーがあれば再起動する必要があ

ります。例えば、PingFederate を使った高可用性の構成でない場合は STANDALONE を使用することができます。

PingFederate でプロビジョニングを設定するには

1. PingFederate 管理コンソールにサインオンします。
2. ページ上部の [Applications] (アプリケーション) を選択し、[SP Connections] (SP 接続) をクリックします。
3. IAM Identity Center との SAML 接続を形成するために前回作成したアプリケーションを検索して、接続名をクリックします。
4. ページの上部にある暗いナビゲーションの見出しから [Connection Type] (接続タイプ) を選択します。前回の SAML の設定で、Browser SSO が既に選択されているはずです。選択されていない場合は、先にその手順を完了させてから次に進みます。
5. [アウトバウンドプロビジョニング] チェックボックスを選択して、タイプとして [IAM Identity Center クラウドコネクター] を選択して、[保存] をクリックします。[IAM Identity Center Cloud Connector] がオプションとして表示されない場合は、IAM Identity Center がインストールされていることを確認して、PingFederate サーバーを再起動します。
6. [Outbound Provisioning] (アウトバウンドプロビジョニング) ページが表示されるまで、繰り返し [Next] (次へ) をしクリックします。ページが表示されたら、[Configure Provisioning] (プロビジョニングの設定) ボタンをクリックします。
7. 前の手順で、IAM Identity Center から [SCIM エンドポイント] の値をコピーしました。その値を PingFederate コンソールの [SCIM URL] フィールドに貼り付けます。URL の末尾にあるスラッシュを削除してください。また、前の手順で、IAM Identity Center の [アクセストークン] の値をコピーしました。その値を PingFederate コンソールの [アクセストークン] フィールドに貼り付けます。[Save] (保存) をクリックします。
8. [Channel Configuration (Configure Channels)] (チャンネル設定 (チャンネルの設定)) ページで [Create] (作成) をクリックします。
9. 新しいプロビジョニングチャネルのチャネル名 (**`AWSIAMIdentityCenterchannel`** など) を入力し、[Next] (次へ) をクリックします。
10. [ソース] ページでは、IAM Identity Center への接続に使用する [アクティブデータストア] を選択し、[次へ] をクリックします。

> **Note**
>
> データソースを設定していない場合は、すぐに設定する必要があります。Ping でのデータソースの選択と設定方法については、PingFederate 製品のドキュメントを参照してください。

11. [Source Settings] (ソースの設定) ページで、すべての値がインストールに対して正しいことを確認して、[Next] (次へ) をクリックします。
12. [Source Location] (ソースの場所) ページで、データソースに適した設定を入力して、[Next] (次へ) をクリックします。例えば、アクティブディレクトリを LDAP ディレクトリとして使用する場合などです。

    a. AD フォレストのベース DN を入力します (例: **`DC=myforest,DC=mydomain,DC=com`**)。

    b. [ユーザー] > [グループ DN] を選択して、IAM Identity Center にプロビジョニングしたいすべてのユーザーを含む単一のグループを指定します。単一のグループが存在しない場合は、AD にグループを作成してからこの設定に戻って、対応する DN を入力します。

    c. サブグループを検索するかどうか (ネスト検索) と、必要な LDAP フィルターを指定します。

    d. [グループ] > [グループ DN] を選択して、IAM Identity Center にプロビジョニングしたいすべてのグループを含む単一のグループを指定します。通常、これは [Users] (ユーザー) セクションで指定したのと同じ DN である可能性があります。必要に応じて ネスト検索とフィルターの値を入力します。

13. [Attribute Mapping] (属性マッピング) ページで以下の項目を確認し、[Next] (次へ) をクリックします。

    a. [userName] フィールドは、E メールとしてフォーマットされた属性にマッピングされている必要があります (user@domain.com)。また、ユーザーが Ping にログインする際に使用する値と一致していなければなりません。この値は、フェデレーション認証の際に SAML `nameId` クレームに入力され、IAM Identity Center でのユーザーとのマッチングに使用されます。例えば、アクティブディレクトリを使用している場合、userName に `UserPrincipalName` を指定することができます。

    b. サフィックスに * が付いているその他のフィールドは、ユーザーの NULL 以外の属性にマップする必要があります。

14. [Activation & Summary] (アクティベーションとサマリー) ページで、[Channel Status] (チャネルステータス) を Active (アクティブ) に設定すると、保存するとすぐに同期が開始されます。

15. ページ上の設定値がすべて正しいことを確認して、[Done] (完了) をクリックします。
16. [Manage Channels] (チャネルの管理) ページで [Save] (保存) をクリックします。
17. この時点で、プロビジョニングが開始します。アクティビティは、provisioner.log ファイルで確認できます。デフォルトでは PingFederate サーバーの pingfederate-<version>/pingfederate/log ディレクトリに保存されています。
18. ユーザーおよびグループが IAM Identity Center にすべて正常に同期されたことを確認するには、 IAM Identity Center コンソールに戻り、[Users] (ユーザー) を選択します。PingFederate から同期されたユーザーは、[ユーザー] ページに表示されます。また、同期したグループは [Groups] (グループ) ページで確認できます。

(オプション) ステップ 3: IAM Identity Center でのアクセスコントロール用に PingFederate でユーザー属性を設定する

これは、AWS リソースへのアクセスを管理するために IAM Identity Center の属性設定を選択した場合の PingFederate のオプション手順です。PingFederate で定義した属性は、SAML アサーションで IAM Identity Center に渡されます。その後、IAM Identity Center でアクセス権限セットを作成し、PingFederate から渡された属性に基づいてアクセスを管理します。

この手順を始める前に、最初に アクセスコントロールの属性 機能を有効にしておく必要があります。これを行う方法については、「アクセスコントロールのための属性の有効化と設定」を参照してください。

IAM Identity Center でのアクセスコントロールに使用される PingFederate の属性の有効化と設定

1. PingFederate 管理コンソールにサインオンします。
2. ページ上部の [Applications] (アプリケーション) を選択し、[SP Connections] (SP 接続) をクリックします。
3. IAM Identity Center との SAML 接続を形成するために前回作成したアプリケーションを検索して、接続名をクリックします。
4. ページの上部にある暗いナビゲーションの見出しから [Browser SSO] (ブラウザ SSO) を選択します。次に [Configure Browser SSO] (ブラウザ SSO の設定) をクリックします。
5. [Configure Browser SSO] (ブラウザ SSO の設定) ページで、[Assertion Creation] (アサーションの作成) を選択し、[Configure Assertion Creation] (アサーション作成の設定) をクリックします。
6. [Configure Assertion Creation] (アサーション作成の設定) ページで、[Attribute Contract] (属性契約) を選択します。

7. [Attribute Contract] (属性の契約) ページの [Extend the Contract] (契約の拡張) セクションで、以下の手順で新しい属性を追加します。

   a. テキストボックスには `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`AttributeName`** を入力し、**`AttributeName`** は IAM Identity Center で想定している属性名に置き換えます。例えば、「`https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Department`**」と入力します。

   b. [属性名の形式] では、[urn:oasis:names:tc:SAML:2.0:attrname-format:uri] を選択します。

   c. [Add] (追加) を選択して、次に [Next] (次へ) を選択します。

8. [Authentication Source Mapping] (認証ソースマッピング) ページで、アプリケーションに設定されているアダプタインスタンスを選択します。

9. [Attribute Contract Fulfillment] (属性契約の履行) ページで、[Attribute Contract] (属性契約) `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Department`** の [Source] (ソース) (data store (データストア)) と [Value] (値) (data store attribute (データストア属性)) を選択します。

   > **Note**
   >
   > データソースを設定していない場合は、すぐに設定する必要があります。Ping でのデータソースの選択と設定方法については、PingFederate 製品のドキュメントを参照してください。

10. [Activation & Summary] (アクティベーションとサマリー) ページが表示されるまで、繰り返し [Next] (次へ) をクリックします。ページが表示されたら、[Save] (保存) をクリックします。

(オプション) アクセスコントロールの属性を渡す

IAM Identity Center の アクセスコントロールの属性 機能をオプションで使用して、Name 属性を `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`** に設定した `Attribute` 要素を渡すことができます。この要素を使用すると、SAML アサーションでセッションタグとして属性を渡すことができます。セッションタグの詳細については、「IAM ユーザーガイド」の「AWS STS でのタグ付けの規則 」 を参照してください。

属性をセッションタグとして渡すには、タグの値を指定する `AttributeValue` 要素を含めます。例えば、タグのキーバリューのペア `CostCenter = blue` を渡すには、次のような属性を使用します。

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

複数の属性を追加する必要がある場合は、各タグに個別の `Attribute` 要素を含めます。

PingOne

IAM Identity Center は、Ping Identity(以下、Ping) の PingOne 製品から IAM Identity Center へのユーザー情報の自動プロビジョニング (同期化) をサポートしています。このプロビジョニングでは、クロスドメインアイデンティティ管理システム (SCIM) v2.0 プロトコルを使用します。この接続を PingOne で設定するには、IAM Identity Center SCIM エンドポイントとアクセストークンを使用します。SCIM 同期を設定すると、PingOne のユーザー属性と IAM Identity Center の名前付き属性のマッピングが作成されます。これにより、IAM Identity Center と PingOne の間で、期待される属性が一致します。

このガイドは、2020 年 10 月時点の PingOne に基づいています。新しいバージョンでは、手順が異なる場合があります。他のバージョンの Ping の IAM Identity Center へのプロビジョニングの設定方法の詳細については、PingOne にお問い合わせください。また、このガイドには、SAML によるユーザー認証の設定に関するいくつかの注意事項が記載されています。

次のステップでは、SCIM プロトコルを使用して、PingOne から IAM Identity Center へのユーザーとグループの自動プロビジョニングを有効にする方法を説明します。

> **Note**
>
> SCIM のデプロイを開始する前に、まず 自動プロビジョニングを使用する際の注意事項 を確認することをお勧めします。そして、次のセクションで残りの注意事項を確認します。

トピック

- (オプション) ステップ 3: IAM Identity Center でのアクセスコントロールのために PingOne でユーザー属性を設定する
- (オプション) アクセスコントロールの属性を渡す

前提条件

開始する前に、以下の準備が必要です。

- フェデレーション認証とプロビジョニング機能の両方を備えた PingOne のサブスクリプションまたは無料トライアル。無料トライアルの取得方法の詳細については、Ping Identityウェブサイトを参照してください。
- IAM Identity Center 対応アカウント (無料)。詳細については、「IAM Identity Center の有効化」を参照してください。
- PingOneIAM ID センターアプリケーションがPingOne管理ポータルに追加されました。PingOneIAM Identity Center アプリケーションはPingOneアプリケーションカタログから入手できます。一般的な情報については、Ping Identity ウェブサイトの「アプリケーションカタログからアプリケーションを追加する」を参照してください。
- PingOne インスタンスから IAM Identity Center への SAML 接続。PingOneIAM Identity Center アプリケーションが、PingOne管理者ポータルに追加されたら、そのアプリケーションを使用して、PingOneインスタンスから IAM Identity Center への SAML 接続を設定する必要があります。両端のメタデータの「ダウンロード」および「インポート」機能を使用して、PingOne と IAM Identity Center 間で SAML メタデータを交換します。この接続を設定する手順については、PingOne のドキュメントを参照してください。

追加の考慮事項

以下は、IAM Identity Center によるプロビジョニングの実装方法に影響を与える可能性がある PingOne に関する重要な注意事項です。

- 2020 年 10 月時点で、PingOne は SCIM によるグループのプロビジョニングをサポートしていません。Ping の SCIM のグループサポートに関する最新情報については、PingOne にお問い合わせください。
- PingOne 管理者ポータルでプロビジョニングを無効にしても、PingOne からユーザーのプロビジョニングが継続される場合があります。プロビジョニングをすぐに終了する必要がある場合は、該当する SCIM ベアラートークンを削除するか、IAM Identity Center の 自動プロビジョニング を無効にします。

- ユーザーの属性が PingOne で設定されたデータストアから削除されても、IAM Identity Center の対応するユーザーからはその属性は削除されません。これは、PingOne's のプロビジョナーの実装における既知の制限です。属性が変更された場合、その変更は IAM Identity Center に同期されます。
- 以下は、PingOne での SAML 設定に関する重要な注意事項です。
  - IAM Identity Center は `NameId` 形式として `emailaddress` のみサポートします。これは、PingOne の SAML_SUBJECT マッピングのために、PingOne のディレクトリ内で一意であり、NULL 以外で、E メール/UPN としてフォーマットされた (例えば、user@domain.com) ユーザー属性を選択する必要があるということです。E メール (仕事用) は、 のPingOne内部ディレクトリを使ったテスト構成に使用するのに適した値です。
  - PingOne で + 文字を含むメールアドレスを使用しているユーザーが IAM Identity Center にサインインできず、`'SAML_215'` や `'Invalid input'` などのエラーが発生することがあります。この問題を解決するには、PingOne で、[属性マッピング] の [SAML_SUBJECT] マッピングで [詳細] オプションを選択します。次に、[SP に送信する名前 ID フォーマット:] をドロップダウンメニューで「urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress」に設定します。

ステップ 1: IAM Identity Center でプロビジョニングを有効にする

この最初のステップでは、IAM Identity Center コンソールを使用して、自動プロビジョニングを有効にします。

IAM Identity Center で自動プロビジョニングを有効にするには

1. 前提条件が整ったら、IAM Identity Center コンソールを開きます。
2. 左側のナビゲーションペインの [Settings] (設定) を選択します。
3. [設定] ページで、[自動プロビジョニング] 情報ボックスを探し、[有効化] を選択します。これにより、すぐに IAM Identity Center の自動プロビジョニングが有効になり、必要なエンドポイントとアクセストークンの情報が表示されます。
4. [Inbound automatic provisioning] (インバウンド自動プロビジョニング) ダイアログボックスで、以下のオプションの値をそれぞれコピーします。これらは、後で IdP でプロビジョニングを設定する際に貼り付ける必要があります。
   a. SCIM エンドポイント
   b. アクセストークン
5. [Close] (閉じる) を選択します。

IAM Identity Center でプロビジョニングを設定したので、PingOne IAM Identity Center アプリケーションを使用して残りのタスクを完了する必要があります。これらのステップについて、次の手順で説明します。

ステップ 2: PingOne でプロビジョニングを設定する

PingOne IAM Identity Center アプリケーションで以下の手順を使用して、IAM Identity Center によるプロビジョニングを有効にします。この手順では、PingOne IAM Identity Center アプリケーションがPingOne管理ポータルに既に追加されていることを前提としています。まだ実行していない場合は、「前提条件」を参照してから、この手順を実行して SCIM プロビジョニングを設定してください。

PingOne でプロビジョニングを設定するには

1. PingOne の SAML 設定でインストールした PingOne IAM Identity Center アプリケーションを開きます ([アプリケーション] > [マイアプリケーション])。前提条件 を参照してください。
2. ページの下部までスクロールします。[User Provisioning] (ユーザープロビジョニング) では、[Complete] (完了) リンクを選択して、接続のユーザープロビジョニング構成に移動します。
3. [Provisioning Instructions] (プロビジョニング手順) ページで、[Continue to Next Step] (次のステップに進む) を選択します。
4. 前の手順で、IAM Identity Center から [SCIM エンドポイント] の値をコピーしました。その値をPingOne IAM Identity Center アプリケーションの「SCIM URL」フィールドに貼り付けます。URL の末尾にあるスラッシュを削除してください。また、前の手順で、IAM Identity Center の [アクセストークン] の値をコピーしました。その値をPingOne IAM Identity Center アプリケーションの「ACCESS_TOKEN」フィールドに貼り付けます。
5. [REMOVE_ACTION] では、[Disabled] または [Delete] のいずれかを選択します (詳細はページの説明を参照してください)。
6. [Attribute Mapping] (属性マッピング) ページでは、このページで紹介した 追加の考慮事項 のガイダンスに従って、SAML_SUBJECT (`NameId`) アサーションに使用する値を選択します。[Next] (次へ) を選択して続行します。
7. [PingOne アプリケーションのカスタマイズ - IAM Identity Center] ページで、必要なカスタマイズの変更を行い (オプション)、[次のステップに進む] をクリックします。
8. [グループアクセス] ページでは、プロビジョニングと IAM Identity Center へのシングルサインオンを有効にするユーザーを含むグループを選択します。[Continue to Next Step] (次のステップに進む) を選択します。
9. ページの下部までスクロールして、[Finish] (完了) を選択してプロビジョニングを開始します。

10. ユーザーが IAM Identity Center に正常に同期されたことを確認するには、IAM Identity Center コンソールに戻り、[ユーザー] を選択します。PingOne から同期されたユーザーは、[ユーザー] ページに表示されます。これらのユーザーは、IAM Identity Center 内のアカウントおよびアプリケーションに割り当てられるようになりました。

    PingOne は SCIM によるグループやグループメンバーシップのプロビジョニングをサポートしていないことに注意してください。詳細については、Ping にお問い合わせください。

(オプション) ステップ 3: IAM Identity Center でのアクセスコントロールのために PingOne でユーザー属性を設定する

これは、AWS リソースへのアクセスを管理するために IAM Identity Center の属性設定を選択した場合の PingOne のオプション手順です。PingOne で定義した属性は、SAML アサーションで IAM Identity Center に渡されます。その後、IAM Identity Center でアクセス権限セットを作成し、PingOne から渡された属性に基づいてアクセスを管理します。

この手順を始める前に、最初に アクセスコントロールの属性 機能を有効にしておく必要があります。これを行う方法については、「アクセスコントロールのための属性の有効化と設定」を参照してください。

IAM Identity Center でのアクセスコントロールに使用される PingOne の属性の有効化と設定

1. PingOne の SAML 設定でインストールした PingOne IAM Identity Center アプリケーションを開きます (アプリケーション > マイアプリケーション)。
2. [Edit] (編集) を選択し、[Continue to Next Step] (次のステップに進む) を選択すると、[Attribute Mappings] (属性マッピング) ページが表示されます。
3. [Attribute Mappings] (属性マッピング) ページで [Add new attribute] (新規属性の追加) を選択し、以下の操作を行います。これらの手順は、IAM Identity Center でのアクセスコントロールに使用するために追加する各属性について行う必要があります。

    a. [Application Attribute] (アプリケーション属性) フィールドに `https://aws.amazon.com/SAML/Attributes/AccessControl:`*`AttributeName`* と入力します。*`AttributeName`* を IAM Identity Center で想定している属性名に置き換えます。例えば、「`https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Email`**」と入力します。

    b. [ID ブリッジ属性またはリテラル値] フィールドで、PingOne ディレクトリからユーザー属性を選択します。例えば、E メール (仕事用)。
4. [Next] (次へ) を数回選択して、次に [Finish] (完了) を選択します。

(オプション) アクセスコントロールの属性を渡す

IAM Identity Center の アクセスコントロールの属性 機能をオプションで使用して、Name 属性を `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` に設定した Attribute 要素を渡すことができます。この要素を使用すると、SAML アサーションでセッションタグとして属性を渡すことができます。セッションタグの詳細については、「IAM ユーザーガイド」の「AWS STS でのタグ付けの規則 」 を参照してください。

属性をセッションタグとして渡すには、タグの値を指定する AttributeValue 要素を含めます。例えば、タグのキーバリューのペア `CostCenter = blue` を渡すには、次のような属性を使用します。

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

複数の属性を追加する必要がある場合は、各タグに個別の Attribute 要素を含めます。

IAM アイデンティティセンターで一般的なタスクを開始する

IAM アイデンティティセンターを初めて使用する場合、サービスの使用を開始するための基本的なワークフローは次のとおりです。

1. IAM Identity Center の組織インスタンスを使用している場合は管理アカウントのコンソールにサインインし、IAM Identity Center のアカウントインスタンスを使用している場合 AWS アカウントは にサインインし、IAM Identity Center コンソールに移動します。
2. IAM アイデンティティセンターコンソールから、ユーザーおよびグループの ID を保存するために使用するディレクトリを選択します。IAM アイデンティティセンターには、ユーザーアクセスを設定するために使用できるディレクトリがデフォルトで用意されています。別の ID ソースを使用する場合は、Active Directory または外部 ID プロバイダーに接続できます。
3. 組織インスタンスの場合は、組織内のアカウントを選択し、ディレクトリからユーザーまたはグループ、およびそれらに付与するアクセス許可を選択して、AWS アカウントにユーザーアクセスを割り当てます。
4. 次の方法でユーザーにアプリケーションへのアクセス権を付与します。
   a. お客様が管理する SAML 2.0 アプリケーションをセットアップするには、アプリケーションカタログから事前に統合されているアプリケーションの 1 つを選択するか、独自の SAML 2.0 アプリケーションを追加します。
   b. アプリケーションのプロパティを設定します。
   c. アプリケーションにユーザーアクセスを割り当てます。個々のユーザーアクセス許可を追加するのではなく、グループメンバーシップを通じてユーザーアクセスを割り当てることをお勧めします。グループを使用すると、個々のユーザーにこれらのアクセス権限を適用するのではなく、ユーザーグループに対してアクセス権限を付与または拒否できます。ユーザーが別の組織に異動した場合、そのユーザーを別のグループに移動させるだけです。その後、ユーザーは新しい組織に必要な権限を自動的に受け取ります。
5. デフォルトの IAM Identity Center ディレクトリを使用している場合は、 AWS アクセスポータルにサインインする方法をユーザーに指示します。IAM Identity Center の新規ユーザーは、 AWS アクセスポータルへのサインインに使用する前に、ユーザー認証情報をアクティブ化する必要があります。詳細については、「 ユーザーガイド」の AWS 「 アクセスポータルにサインインするAWS サインイン 」を参照してください。

このセクションのトピックは、IAM アイデンティティセンターの初期設定が完了した後に実行される一般的なタスクを理解するのに役立ちます。

IAM アイデンティティセンターをまだ有効にしていない場合は、「の有効化 AWS IAM Identity Center」を参照してください。

トピック

- アクセス権限セットを作成します。
- IAM Identity Center ユーザーに AWS アカウント アクセス権を割り当てる
- IAM Identity Center の認証情報を使用して AWS アクセスポータルにサインインする
- グループに AWS アカウント アクセス権を割り当てる
- アプリケーションへのシングルサインオンアクセスを設定する
- ユーザーとグループの割り当てを表示する

アクセス権限セットを作成します。

権限セットは IAM Identity Center に保存され、ユーザーおよびグループが持つこの AWS アカウントに対するアクセスのレベルを定義します。最初に作成するアクセス許可セットは管理許可セットです。入門チュートリアル のいずれかを完了した場合は、管理許可セットは作成済みです。「IAM ユーザーガイド」の「職務機能のAWS マネージドポリシー」のトピックで説明されているように、この手順を使用してアクセス許可セットを作成します。

1. 以下のいずれかを行って、 AWS Management Consoleにサインインします。
   - 新規ユーザー AWS （ルートユーザー） – ルートユーザーを選択し、 AWS アカウント E メールアドレスを入力して、アカウント所有者としてサインインします。次のページでパスワードを入力します。
   - （ AWS IAM 認証情報) を既に使用 – 管理者権限を持つ IAM 認証情報を使用してサインインします。
2. IAM Identity Center コンソールを開きます。
3. IAM Identity Center のナビゲーションペインの「マルチアカウント権限」で、「アクセス権限セット」を選択します。
4. [Create permission set] (アクセス権限セットの作成) を選択します。
   a. 「アクセス権限セットタイプの選択」ページの「アクセス権限セットタイプ」セクションで、「定義済みのアクセス権限セット」を選択します。

b. [事前定義された許可セットのポリシー] セクションで、次のいずれかを選択します。

- AdministratorAccess
- 「請求」
- DatabaseAdministrator
- DataScientist
- NetworkAdministrator
- PowerUserAccess
- ReadOnlyAccess
- SecurityAudit
- SupportUser
- SystemAdministrator
- ViewOnlyAccess

5. [アクセス権限セットの詳細を指定] ページでは、デフォルト設定のまま [次へ] を選択します。デフォルト設定では、セッションは 1 時間に制限されています。
6. [確認と作成] ページで、次のことを確認します。

1. ステップ 1: アクセス許可セットタイプ を選択する では、選択したアクセス許可セットのタイプが表示されます。
2. ステップ 2: アクセス許可セットの詳細を定義するには、選択したアクセス許可セットの名前を に表示します。
3. [作成] を選択します。

最小特権権のアクセス許可を適用するアクセス許可セットを作成する

最小特権のアクセス許可を適用するというベストプラクティスに従うには、管理権許可セットを作成した後に、より制限の厳しいアクセス許可セットを作成して 1 人以上のユーザーに割り当てます。前の手順で作成したアクセス許可セットは、ユーザが必要とするリソースへのアクセス量を評価するための出発点となります。最小特権のアクセス許可に切り替えるには、IAM Access Analyzer を実行して、 AWS マネージドポリシーを持つプリンシパルをモニタリングできます。どのアクセス許可を使用しているかがわかったら、カスタムポリシーを作成するか、チームに必要なアクセス許可のみを持つポリシーを生成します。

IAM Identity Center を使用すると、同じユーザーに複数のアクセス権限セットを割り当てることができます。管理ユーザーには、より制限の厳しいアクセス許可セットを追加で割り当てる必要もあります。これにより、常に管理アクセス許可を使用するのではなく、必要なアクセス許可のみ AWS アカウント を使用して にアクセスできます。

例えば、開発者の場合、IAM アイデンティティセンターで管理ユーザーを作成した後に、PowerUserAccess アクセス許可を付与する新しいアクセス許可セットを作成し、そのアクセス許可セットを自身に割り当てることができます。アクセス許可を使用する管理AdministratorAccessアクセス許可セットとは異なり、アクセスPowerUserAccess 許可セットでは IAM ユーザーとグループの管理が許可されません。 AWS アクセスポータルにサインインして AWS アカウントにアクセスすると、 PowerUserAccessではなく を選択してアカウントで開発タスクAdministratorAccessを実行できます。

次の考慮事項に注意が必要です。

- より制限の厳しいアクセス権限セットをすぐに作成するには、カスタムアクセス権限セットではなく定義済みのアクセス権限セットを使用してください。

  定義済みのアクセス許可を使用する定義済みのアクセス許可セットでは、使用可能なポリシーのリストから 1 つの AWS 管理ポリシーを選択します。各ポリシーは、 AWS サービスおよびリソースへの特定のレベルのアクセス、または共通の職務機能に対するアクセス許可を付与します。これらのポリシーそれぞれの詳細については、「AWS 職務機能の管理ポリシー」を参照してください。
- アクセス権限セットのセッション期間を構成して、ユーザーが AWS アカウントにサインインしている時間を制御できます。

  ユーザーが にフェデレーション AWS アカウント し、 AWS マネジメントコンソールまたは AWS コマンドラインインターフェイス (AWS CLI) を使用する場合、IAM Identity Center はアクセス許可セットのセッション期間設定を使用してセッション期間を制御します。デフォルトでは、セッション期間 の値は、ユーザーがセッションから AWS サインアウト AWS アカウント するまでにサインインできる時間の長さを決定するもので、1 時間に設定されます。最大値は 12 時間まで指定できます。詳細については、「セッション期間の設定」を参照してください。
- AWS アクセスポータルのセッション期間を設定して、ワークフォースユーザーがポータルにサインインする期間を制御することもできます。

  デフォルトでは、最大セッション期間 の値は、ワークフォースユーザーが再認証される前に AWS アクセスポータルにサインインできる時間の長さを決定し、8 時間です。最大値は 90 日まで指定できます。詳細については、「AWS アクセスポータルと IAM Identity Center 統合アプリケーションのセッション期間を設定する」を参照してください。

- AWS アクセスポータルにサインインするときは、最小特権のアクセス許可を付与するロールを選択します。

  作成してユーザーに割り当てる各アクセス許可セットは、 AWS アクセスポータルで使用可能なロールとして表示されます。そのユーザーとしてポータルにサインインするときは、アカウント内のタスクの実行に使用できる最も制限の厳しいアクセス権限セットに対応するロールを (`AdministratorAccess` ではなく) 選択してください。

- IAM Identity Center に他のユーザーを追加し、そのユーザーに既存または新規のアクセス権限セットを割り当てることができます。

  詳細については、「グループに AWS アカウント アクセス権を割り当てる」を参照してください。

IAM Identity Center ユーザーに AWS アカウント アクセス権を割り当てる

IAM Identity Center ユーザーの AWS アカウント アクセスを設定するには、 AWS アカウント および アクセス許可セットにユーザーを割り当てる必要があります。

1. 以下のいずれかを行って、 AWS Management Consoleにサインインします。

   - 新規ユーザー AWS （ ルートユーザー ） – ルートユーザーを選択し、 AWS アカウント E メールアドレスを入力して、アカウント所有者としてサインインします。次のページでパスワードを入力します。
   - （ AWS IAM 認証情報) を既に使用 – 管理者権限を持つ IAM 認証情報を使用してサインインします。

2. IAM Identity Center コンソール を開きます。
3. ナビゲーションペインの [マルチアカウント権限] で、AWS アカウント を選択します。
4. AWS アカウント ページには、組織のツリービューリストが表示されます。アクセス AWS アカウント を割り当てる の横にあるチェックボックスをオンにします。IAM アイデンティティセンターの管理アクセスを設定する場合は、管理アカウントの横にあるチェックボックスをオンにします。
5. 「ユーザーまたはグループを割り当て」を選択します。
6. ステップ 1: ユーザーとグループ を選択するには、***AWS ##### #####***とグループを」に割り当てるページで、次の操作を行います。

1. [ユーザー] タブで、管理者権限を付与するユーザーを選択します。

   結果をフィルタリングするには、検索ボックスに目的のユーザーの名前を入力します。

2. 正しいユーザーが選択されていることを確認したら、[次へ] を選択します。

7. ステップ 2: アクセス許可セット を選択するには、アクセス許可セットを*AWS ##### ###*」ページ、アクセス許可セット でアクセス許可セットを選択して、この に対するユーザーとグループのアクセスレベルを定義します AWS アカウント。
8. [次へ] をクリックします。
9. ステップ 3: を確認して送信するには、「名前*AWS ##### *」ページから、次の操作を行います。

   1. 選択したユーザーとアクセス権限セットを確認します。
   2. 正しいユーザーがアクセス許可セットに割り当てられていることを確認したら、「送信」を選択します。

   > **Important**
   >
   > ユーザーへの割り当てプロセスが完了するまでに数分かかることがあります。プロセスが正常に完了するまで、このページを開いたままにしておきます。

10. 以下のいずれかに当てはまる場合は、ユーザーに MFA を求める の手順に従って IAM Identity Center の MFA を有効にしてください。

    - ID ソースとしてデフォルトの Identity Center ディレクトリを使用しています。
    - Active Directory の AWS Managed Microsoft AD ディレクトリまたはセルフマネージドディレクトリを ID ソースとして使用しており、 で RADIUS MFA を使用していません AWS Directory Service。

    > **Note**
    >
    > 外部 ID プロバイダーを使用している場合は、IAM Identity Center ではなく外部 IdP が MFA 設定を管理することに注意してください。IAM Identity Center の MFA は、外部 では使用できません IdPs。

管理ユーザーのアカウントへのアクセス権をセットアップすると、対応する IAM ロールが IAM Identity Center により作成されます。このロールは IAM Identity Center によって制御され、関連するで作成され AWS アカウント、アクセス許可セットで指定されたポリシーがロールにアタッチされます。

IAM Identity Center の認証情報を使用して AWS アクセスポータルにサインインする

AWS アクセスポータルでは、IAM Identity Center ユーザーは、ウェブポータルを通じて、割り当てられたすべての AWS アカウント およびアプリケーションへのシングルサインオンアクセスが可能になります。

以下の手順を実行して、IAM Identity Center ユーザーが AWS アクセスポータルにサインインして にアクセスできることを確認します AWS アカウント。

1. 以下のいずれかを行って、 AWS Management Consoleにサインインします。

   - 新規ユーザー AWS （ルートユーザー） – ルートユーザーを選択し、 AWS アカウント E メールアドレスを入力して、アカウント所有者としてサインインします。次のページでパスワードを入力します。
   - （ AWS IAM 認証情報) を既に使用 – IAM 認証情報を使用してサインインし、管理者ロールを選択します。

2. IAM Identity Center コンソール を開きます。
3. ナビゲーションペインで、ダッシュボード を選択します。
4. ダッシュボードページの「設定の概要」で、 AWS アクセスポータル URL を選択します。
5. 次のいずれかを使用してサインインします。

   - Active Directory または外部 ID プロバイダー (IdP) を ID ソースとして使用している場合は、Active Directory または IdP ユーザーの認証情報でサインインします。
   - ID ソースとしてデフォルトの Identity Center ディレクトリを使用している場合は、ユーザーを作成したときに指定したユーザー名と、そのユーザーに指定した新しいパスワードを使用してサインインします。

1. アカウント タブで、 を見つけ AWS アカウント て展開します。

2. 使用可能なロールが表示されます。例えば、アクセスAdministratorAccess権限セットと請求権限セットの両方が割り当てられている場合、それらのロールは AWS アクセスポータルに表示されます。セッションに使用する IAM ロール名を選択します。
3. AWS マネジメントコンソールにリダイレクトされると、 へのアクセスの設定が正常に完了しました AWS アカウント。

> **Note**
>
> AWS アカウント一覧に何も表示されない場合は、そのユーザはそのアカウントのアクセス権限セットにまだ割り当てられていない可能性があります。アクセス権限セットにユーザを割り当てる手順については、へのユーザーアクセスを割り当てる AWS アカウント を参照してください。

IAM Identity Center の認証情報を使用してサインインできることを確認したので、 へのサインインに使用したブラウザに切り替え AWS Management Console 、ルートユーザーまたは IAM ユーザーの認証情報からサインアウトします。

> **Important**
>
> アクセス AWS ポータルにサインインするときは、IAM ユーザーまたはルートユーザーの認証情報を使用する代わりに、IAM Identity Center 管理ユーザーの認証情報を使用して管理タスクを実行することを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。他のユーザーがアカウントやアプリケーションにアクセスできるようにし、IAM Identity Center を管理できるようにするには、IAM Identity Center を通じてのみアクセス権限セットを作成して割り当ててください。

グループに AWS アカウント アクセス権を割り当てる

IAM Identity Center で管理ユーザーを作成し、最小特権のアクセス許可を持つタスクの実行に使用できる追加のアクセス許可セットを作成したら、 へのアクセス AWS アカウント をユーザーグループに提供できます。

個々のユーザーではなくグループに直接アクセスを割り当てることをお勧めします。例えば、組織単位に基づいてグループとアクセス許可セットを作成した場合、ユーザーが別の組織単位に移動する

と、そのユーザーが別のグループに移動するだけで、新しい組織単位に必要なアクセス許可が自動的に割り当てられ、以前の組織単位のアクセス許可は失われます。

へのユーザーグループアクセスを割り当てるには AWS アカウント

1. IAM Identity Center コンソールを開きます。

   > **Note**
   >
   > ID ソースが の場合、次のステップに進む前に、IAM Identity Center コンソールで AWS Managed Microsoft AD ディレクトリがあるリージョンを使用し AWS Managed Microsoft AD ていることを確認してください。

2. ナビゲーションペインの [マルチアカウントのアクセス許可] で、[AWS アカウント] を選択します。
3. [AWS アカウント] ページには、組織のツリービューリストが表示されます。シングルサインオンアクセスを割り当てる 1 つ以上の AWS アカウント の横にあるチェックボックスをオンにします。

   > **Note**
   >
   > アクセス許可セット AWS アカウント ごとに最大 10 個まで選択できます。

4. 「ユーザーまたはグループを割り当て」を選択します。
5. [ステップ 1: ユーザーとグループの選択] では、[ユーザーとグループを ***AWS-account-name*** に割り当てる] ページで [グループ] タブを選択後、1 つまたは複数のグループを選択します。

   結果をフィルターする場合は、検索ボックスに目的のグループの名前を入力します。

   選択したグループを表示するには、[選択したユーザーとグループ] の横にある横向きの三角形を選択します。

   正しいグループが選択されたことを確認したら、[次へ] を選択します。
6. [ステップ 2: アクセス許可セットの選択] では、[アクセス許可セットを "***AWS-account-name***" に割り当てる] ページで 1 つ以上のアクセス許可セットを選択します。

> **Note**
>
> この手順を開始する前に必要なアクセス許可セットを作成していない場合は、[許可セットを作成] を選択し、アクセス権限セットを作成します。 の手順に従ってください。適用する権限セットを作成したら、IAM Identity Center コンソールで「AWS アカウント」に戻り、「ステップ 2: 権限セットを選択する」が表示されるまで指示に従います。このステップに到達したら、作成した新しい権限セットを選択し、この手順の次のステップに進みます。

正しい権限セットが選択されていることを確認したら、[次へ] を選択します。

7. ステップ 3: 確認して送信では、「***AWS-account-name***」への課題のレビューと提出ページで、次の操作を行います。

   1. 選択したグループとアクセス許可セットを確認します。
   2. 正しいグループとアクセス許可セットが選択されていることを確認したら、[送信] を選択します。

   > **Important**
   >
   > グループへの割り当てプロセスが完了するまでに数分かかることがあります。プロセスが正常に完了するまで、このページを開いたままにしておきます。

   > **Note**
   >
   > AWS Organizations 管理アカウントで運用するためのアクセス許可をユーザーまたはグループに付与する必要がある場合があります。権限の高いアカウントであるため、追加のセキュリティ制限により、これを設定する前に IAMFullAccess ポリシーまたは同等のアクセス許可が必要です。これらの追加のセキュリティ制限は、 AWS 組織内のメンバーアカウントでは必要ありません。

または、AWS CloudFormation を使用してアクセス権限セットを作成して割り当て、それらのアクセス権限セットにユーザを割り当てることもできます。ユーザーは、AWS アクセスポータルにサインイン するか、AWS Command Line Interface (AWS CLI) コマンドを使用できます。

アプリケーションへのシングルサインオンアクセスを設定する

IAM Identity Center は、マネージドアプリケーションとカスタマーマネージド AWS アプリケーションの 2 つのアプリケーションタイプをサポートしています。

AWS マネージドアプリケーションは、関連するアプリケーションコンソール内から直接、またはアプリケーション APIsを介して設定されます。

カスタマーマネージドアプリケーションは、IAM アイデンティティセンターコンソールに追加され、IAM アイデンティティセンターおよびサービスプロバイダーの両方で適切なメタデータを設定する必要があります。SAML 2.0 をサポートする、よく使用されるアプリケーションのカタログから選択することも、独自の SAML 2.0 アプリケーションまたは OAuth 2.0 アプリケーションをセットアップすることもできます。

アプリケーションへのシングルサインオンアクセスを設定するための設定手順は、アプリケーションの種類によって異なります。

AWS マネージドアプリケーションのセットアップ

AWS Amazon Managed Grafana や Amazon Monitron などの マネージドアプリケーションは IAM Identity Center と統合され、認証およびディレクトリサービスに使用できます。 AWS マネージドアプリケーションを IAM Identity Center と連携するようにセットアップするには、該当するサービスのコンソールから直接アプリケーションを設定するか、アプリケーション APIsを使用する必要があります。

アプリケーションカタログからアプリケーションをセットアップする

IAM アイデンティティセンターコンソールで、よく使用されるアプリケーションのカタログから SAML 2.0 アプリケーションを選択できます。IAM アイデンティティセンターとアプリケーションのサービスプロバイダーとの間で SAML 2.0 の信頼関係を設定するには、以下の手順を実行します。

アプリケーションカタログからアプリケーションをセットアップするには

1. IAM Identity Center コンソール を開きます。
2. [Applications] (アプリケーション) を選択します。
3. [カスタマーマネージド] タブを選択します。
4. [アプリケーションの追加] を選択します。
5. [アプリケーションタイプを選択] ページの [セットアッププリファレンス] で、[カタログからアプリケーションを選択したい] を選択します。

6. [アプリケーションカタログ] で、追加するアプリケーションの名前を検索ボックスに入力し始めます。
7. 検索結果に表示されたら、一覧からアプリケーションの名前を選択し、[次へ] を選択します。
8. [アプリケーションを設定] ページの [表示名] と [説明] フィールドには、アプリケーションに関連する詳細があらかじめ入力されています。この情報は編集することができます。
9. 「IAM Identity Center」で、以下の作業を行います。

   a. IAM Identity Center SAML メタデータファイルの横にある [ダウンロード] を選択して、ID プロバイダーのメタデータをダウンロードします。

   b. [IAM Identity Center 証明書] の横にある [証明書のダウンロード] を選択して、ID プロバイダーの証明書をダウンロードします。

   > **Note**
   >
   > 後で、サービスプロバイダーのウェブサイトからアプリケーションを設定するときに、これらのファイルが必要になります。そのプロバイダーからの手順に従います。

10. (オプション) [アプリケーションプロパティ] の下で、[アプリケーション開始 URL]、[リレー状態]、[セッション期間] を指定できます。詳細については、「IAM アイデンティティセンターコンソールのアプリケーションプロパティを設定する」を参照してください。
11. [Application metadata] (アプリケーションメタデータ) で、以下のいずれかを行います。

    a. メタデータファイルがある場合は、[アプリケーション SAML メタデータファイルをアップロードする] を選択します。次に、[ファイルを選択] を選択してメタデータファイルを検索して選択します。

    b. メタデータファイルがない場合は、[メタデータ値を手動で入力する] を選択して、[アプリケーション ACS URL] および [アプリケーション SAML 対象者] の値を指定します。

12. [送信] を選択します。追加したアプリケーションの詳細ページが表示されます。

独自の SAML 2.0 アプリケーションをセットアップする

IAM アイデンティティセンターとお客様の SAML 2.0 アプリケーションのサービスプロバイダーとの間で独自の SAML 2.0 の信頼関係を設定するには、以下の手順を実行します。この手順を開始する前に、信頼をより効率的に設定できるように、サービスプロバイダーの証明書とメタデータエクスチェンジファイルがあることを確認してください。

独自の SAML 2.0 アプリケーションを設定するには

1. IAM Identity Center コンソール を開きます。
2. [Applications] (アプリケーション) を選択します。
3. [カスタマーマネージド] タブを選択します。
4. [アプリケーションの追加] を選択します。
5. [アプリケーションタイプを選択] ページの [セットアッププリファレンス] で、[セットアップしたいアプリケーションがある] を選択します。
6. [アプリケーションタイプ] で、[SAML 2.0] を選択します。
7. [次へ] をクリックします。
8. [アプリケーションの設定] ページの [アプリケーションの設定] で、**MyApp** のようにアプリケーションの [表示名] を入力します。[Description] を入力します。
9. 「IAM Identity Center」で、以下の作業を行います。
   a. IAM Identity Center SAML メタデータファイルの横にある [ダウンロード] を選択して、ID プロバイダーのメタデータをダウンロードします。
   b. [IAM アイデンティティセンターの証明書] で、[ダウンロード] を選択して、ID プロバイダーの証明書をダウンロードします。

   > **Note**
   >
   > 後で、サービスプロバイダーのウェブサイトからカスタムアプリケーションを設定するときに、これらのファイルが必要になります。

10. (オプション) [アプリケーションプロパティ] の下で、[アプリケーション開始 URL]、[リレー状態]、[セッション期間] も指定できます。詳細については、「IAM アイデンティティセンターコンソールのアプリケーションプロパティを設定する」を参照してください。
11. [アプリケーションメタデータ] で [メタデータの値を手動で入力] を選択します。次に、[アプリケーション ACS URL] および [アプリケーション SAML 対象者] の値を指定します。
12. [送信] を選択します。追加したアプリケーションの詳細ページが表示されます。

アプリケーションを設定すると、ユーザーは割り当てたアクセス許可に基づいて AWS アクセスポータル内からアプリケーションにアクセスできます。

OAuth 2.0 をサポートするカスタマーマネージドアプリケーションがあり、ユーザーがこれらのアプリケーションから AWS サービスにアクセスする必要がある場合は、信頼できる ID の伝播を使用できます。信頼できる ID の伝播を使用すると、ユーザーはアプリケーションにサインインでき、そのアプリケーションは AWS サービスのデータにアクセスするためのリクエストでユーザーの ID を渡すことができます。詳細については、「カスタマーマネージドアプリケーションによる信頼できる ID の伝播の使用」を参照してください。

サポートされているアプリケーションのタイプの詳細については、「アプリケーションへのアクセスの管理」を参照してください。

ユーザーとグループの割り当てを表示する

ユーザーおよびグループページから、IAM Identity Center のモノにアクセスできるユーザーを確認できます。この手順を使用して、ユーザーが AWS アカウント、アクセス許可セット、アプリケーション、およびグループに対して持つアクセスのレベルを表示します。

1. IAM Identity Center コンソールを開きます。
2. ユーザーのグループを編集するか、個別に割り当てられた 1 人のユーザーを編集するかに基づいて、ユーザーまたはグループを選択します。
3. リストからユーザーまたはグループを選択します。
4. アカウント割り当て、アプリケーション割り当て、またはグループ割り当てを表示するかどうかを選択します。

   - AWS アカウントとアクセス許可セットの割り当て
     1. [Accounts] タブを選択します。
     2. リストからアカウントを選択すると、ユーザーとグループのアクセス許可セットの割り当てが表示されます。
     3. ポリシーと割り当ての詳細を表示するアクセス許可セットを選択します。
   - アプリケーション割り当て
     1. アプリケーションタブを選択すると、ユーザーまたはグループに割り当てられるアプリケーションが表示されます。
     2. リストからアプリケーションを選択すると、割り当ての詳細が表示されます。
   - グループ割り当て
     1. ユーザー ページから、グループ タブを選択します。
     2. グループを選択して、ユーザーのグループ割り当てを表示します。

IAM アイデンティティセンターの組織インスタンスとアカウントインスタンスの管理

インスタンスは IAM アイデンティティセンターの単一デプロイです。IAM アイデンティティセンターで使用できるインスタンスには、組織インスタンスとアカウントインスタンスの 2 種類があります。

AWS アカウント IAM Identity Center を有効にできる タイプ

IAM Identity Center を有効にするには、作成するインスタンスタイプに応じて、次のいずれかの認証情報 AWS Management Console を使用して にサインインします。

- AWS Organizations 管理アカウント (推奨) — IAM Identity Center の組織インスタンスを作成するために必要です。組織全体でのマルチアカウント権限とアプリケーションの割り当てには、組織インスタンスを使用してください。
- AWS Organizations メンバーアカウント – IAM Identity Center のアカウントインスタンスを作成して、そのメンバーアカウント内のアプリケーション割り当てを有効にするために を使用します。メンバーレベルのインスタンスを持つ 1 つ以上のアカウントを組織内に持つことができます。
- スタンドアロン AWS アカウント – IAM Identity Center の組織インスタンスまたはアカウントインスタンスを作成するために使用します。スタンドアロン AWS アカウント は によって管理されません AWS Organizations。IAM Identity Center の 1 つのインスタンスのみをスタンドアロンに関連付けることができ AWS アカウント 、そのインスタンスをスタンドアロン 内のアプリケーション割り当てに使用できます AWS アカウント。

機能	AWS Organizations 管理アカウントのインスタンス (推奨)	メンバーアカウント内のインスタンス	スタンドアロンのインスタンス AWS アカウント
ユーザーの管理	 はい	 はい	 はい

機能	AWS Organizations 管理アカウントのインスタンス (推奨)	メンバーアカウント内のインスタンス	スタンドアロンのインスタンス AWS アカウント
AWS AWS マネージドアプリケーションへのシングルサインオンアクセス用の アクセスポータル	 はい	 はい	 はい
OAuth 2.0 (OIDC) カスタマーマネージドアプリケーション	 はい	 はい	 はい
マルチアカウント権限	 はい	 いえ	 いえ
AWS へのシングルサインオンアクセス用の アクセスポータル AWS アカウント	 はい	 いえ	 いえ
SAML 2.0 カスタマーマネージドアプリケーション	 はい	 いえ	 いえ
委任管理者がインスタンスを管理できる	 はい	 いえ	 いえ

トピック

IAM アイデンティティセンターの組織インスタンス

と組み合わせて IAM Identity Center を有効にすると AWS Organizations、IAM Identity Center の組織インスタンスが作成されます。ユーザーとグループのアクセスを 1 つの組織インスタンスで一元管理するには、組織インスタンスは管理アカウントで有効化されている必要があります。 AWS Organizationsでは、各管理アカウントにつき 1 つの組織インスタンスしか作成できません。

2023 年 11 月 15 日より前に IAM アイデンティティセンターを有効にした場合は、IAM アイデンティティセンターの組織インスタンスがあります。

組織インスタンスを使用するタイミング

組織インスタンスは IAM アイデンティティセンターを有効にする主要な方法であり、ほとんどの場合、組織インスタンスが推奨されます。組織インスタンスには、次のような利点があります。

- IAM Identity Center のすべての機能のサポート — 組織 AWS アカウント 内の複数の に対するアクセス許可の管理や、カスタマーマネージドアプリケーションへのアクセスの割り当てが含まれます。
- 管理ポイントの数を減らす — 組織インスタンスには 1 つの管理ポイント、つまり管理アカウントがあります。管理ポイントの数を減らすには、アカウントインスタンスではなく組織インスタンスを有効にすることをお勧めします。
- アカウントインスタンスの作成を制御する – オプトインリージョン (デフォルトでAWS リージョン は無効) の組織に IAM Identity Center のインスタンスをデプロイしていない限り、組織のメンバーアカウントでアカウントインスタンスを作成できるかどうかを制御できます。

IAM アイデンティティセンターのアカウントインスタンス

IAM Identity Center のアカウントインスタンスを使用すると、サポートされている AWS マネージドアプリケーションと OIDC ベースのカスタマーマネージドアプリケーションをデプロイできます。

アカウントインスタンスは、IAM Identity Center のワークフォースアイデンティティとアクセスポータル機能を活用して AWS アカウント、単一の でのアプリケーションの独立したデプロイをサポートします。

アカウントインスタンスは 1 つの にバインド AWS アカウント され、同じアカウントと でサポートされているアプリケーションのユーザーとグループのアクセスを管理するためにのみ使用されます AWS リージョン。ごとに 1 つのアカウントインスタンスに制限されています AWS アカウント。以下のいずれかからアカウントインスタンスを作成できます。

- のメンバーアカウント AWS Organizations。
- によって管理 AWS アカウント されていないスタンドアロン AWS Organizations。

メンバーアカウントの可用性制約

以下の条件に当てはまる場合は、組織のメンバーアカウントにアカウントインスタンスをデプロイできます。

- 2023 年 11 月 15 日より前に組織にデプロイされた IAM Identity Center のインスタンスはありませんでした。
- 2023 年 11 月 15 日より前に IAM Identity Center のインスタンスが組織にデプロイされており、管理者が IAM Identity Center のアカウントインスタンスを作成するメンバーアカウントを有効にしている場合。
- 管理者は、メンバーアカウントがアカウントインスタンスを作成できないようにするサービスコントロールポリシーを作成していません。
- に関係なく、この同じアカウントに IAM Identity Center のインスタンスがまだありません AWS リージョン。
- IAM Identity Center AWS リージョン が利用できない で作業している。リージョンの詳細については、「AWS IAM Identity Center リージョンの可用性」を参照してください。

トピック

- アカウントインスタンスを使用するタイミング
- アカウントインスタンスに関する考慮事項
- AWS アカウントインスタンスをサポートする マネージドアプリケーション

アカウントインスタンスを使用するタイミング

ほとんどの場合には、組織インスタンスをお勧めします。アカウントインスタンスは、以下のシナリオのいずれかに当てはまる場合にのみ使用してください。

- サポートされている AWS マネージドアプリケーションの一時的なトライアルを実行して、アプリケーションがビジネスニーズに適しているかどうかを判断したい。
- 組織全体に IAM Identity Center を導入する予定はありませんが、1 つ以上の AWS マネージドアプリケーションをサポートしたいと考えています。
- IAM Identity Center の組織インスタンスがあるが、サポートされている AWS マネージドアプリケーションを、組織インスタンスのユーザーとは異なる分離されたユーザーのセットにデプロイしたい。

> **Important**
>
> IAM アイデンティティセンターを使用して複数のアカウントのアプリケーションをサポートする予定がある場合は、組織インスタンスを作成し、アカウントインスタンスは使用しないでください。

アカウントインスタンスに関する考慮事項

アカウントインスタンスは特殊なユースケース向けに設計されており、組織インスタンスで使用できる機能のサブセットを提供します。アカウントインスタンスを作成する前に、以下を考慮してください。

- アカウントインスタンスはアクセス許可セットをサポートしていないため、 へのアクセスをサポートしていません AWS アカウント。
- アカウントインスタンスを組織インスタンスに変換することはできません。
- アカウントインスタンスを組織インスタンスにマージすることはできません。
- AWS マネージドアプリケーション サポートアカウントインスタンスのみを選択します。
- アカウントインスタンスは、1 つのアカウントでのみアプリケーションを使用する孤立したユーザーで、使用するアプリケーションの存続期間中だけ使用してください。
- アカウントインスタンスにアタッチされたアプリケーションは、アプリケーションとそのリソースを削除するまでアカウントインスタンスにアタッチされたままにしておく必要があります。

- アカウントインスタンスは、作成された に残 AWS アカウント っている必要があります。

AWS アカウントインスタンスをサポートする マネージドアプリケーション

IAM Identity Center のアカウントインスタンスをサポートする AWS マネージドアプリケーションAWS マネージドアプリケーションについては、「」を参照してください。 AWS マネージドアプリケーションでアカウントインスタンス作成の可用性を検証します。

IAM Identity Center コンソールでアカウントインスタンスを有効にする

2023 年 11 月 15 日より前に IAM Identity Center を有効にした場合、IAM Identity Center の組織インスタンスがあり、メンバーアカウントがアカウントインスタンスを作成する機能はデフォルトで無効になっています。メンバーアカウントがアカウントインスタンスを作成できるかどうかは、 AWS Management Consoleのアカウントインスタンス機能を有効にすることで選択できます。

> **Note**
>
> メンバーアカウントは、デプロイ日に関係なく、オプトインリージョン (デフォルトでは無効) の組織に IAM Identity Center AWS リージョン のインスタンスをデプロイしていない限り、アカウントインスタンスを作成できます。オプトインにデプロイされた IAM Identity Center の組織インスタンスは、アカウントインスタンスの作成を妨げ AWS リージョン ます。リージョンの詳細については、「AWS IAM Identity Center リージョンの可用性」を参照してください。

組織内のメンバーアカウントによるアカウントインスタンスの作成を有効にするには

1. IAM Identity Center コンソールを開きます。
2. [設定] を選択し、[管理] タブを選択します。
3. [IAM アイデンティティセンターのアカウントインスタンス] セクションで、[IAM アイデンティティセンターのアカウントインスタンスを有効にする] を選択します。
4. [IAM アイデンティティセンターのアカウントインスタンスを有効にする] ダイアログボックスで、[有効にする] を選択して、組織内のメンバーアカウントにアカウントインスタンスの作成を許可することを確認します。

> **Important**
>
> メンバーアカウントの IAM Identity Center のアカウントインスタンスを有効にすることは、1 回限りのオペレーションです。つまり、このオペレーションを元に戻すことはできません。有効にすると、サービスコントロールポリシー (SCP) を作成することで、アカウントインスタンスの作成を制限できます。手順については、「サービスコントロールポリシーによるアカウントインスタンスの作成の制御」を参照してください。

サービスコントロールポリシーを使用してアカウントインスタンスの作成を制御する

ユーザーは、IAM Identity Center のアカウントインスタンスと呼ばれる AWS アカウント単一の にバインドされた IAM Identity Center のインスタンスを作成できます。サービスコントロールポリシーを使用してアカウントインスタンスの作成を制御できます。

1. IAM Identity Center コンソールを開きます。
2. [ダッシュボード] の [中央管理] セクションで、[アカウントインスタンスの抑制] ボタンを選択します。
3. [SCP をアタッチして新しいアカウントインスタンスが作成されないようにする] ダイアログボックスに SCP が表示されます。SCP をコピーし、[SCP ダッシュボードに移動] ボタンを選択します。AWS Organizations コンソールに移動し、SCP を作成するか、既存の SCP にステートメントとしてアタッチします。

   サービスコントロールポリシーは の機能です AWS Organizations。SCP をアタッチする手順については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシーのアタッチとデタッチ」を参照してください。

アカウントインスタンスの作成を防ぐのではなく、アカウントインスタンスの作成を組織 AWS アカウント 内の特定の に制限できます。

Example : SCP によるインスタンス作成の制御

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

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

IAM アイデンティティセンターのアカウントインスタンスを作成する

組織インスタンスは IAM アイデンティティセンターを有効にするための主要かつ推奨される方法です。ユースケースがアカウントインスタンスの作成をサポートしていることを確認し、考慮事項を理解していることを確認します。

組織のメンバーアカウントまたはスタンドアロン AWS アカウントからアカウントインスタンスを作成する

1. 以下のいずれかを行って、 AWS Management Consoleにサインインします。
   - 新規ユーザー AWS （ルートユーザー） – ルートユーザーを選択し、 AWS アカウント E メールアドレスを入力して、アカウント所有者としてサインインします。次のページでパスワードを入力します。
   - （ AWS IAM 認証情報) を既に使用 – 管理者権限を持つ IAM 認証情報を使用してサインインします。
2. IAM Identity Center コンソール を開きます。
3. 「IAM Identity Center を有効にする」で、「有効にする」を選択します。
4. [アカウントインスタンスの作成を続行] を選択し、[続行] を選択します。

> **Note**
>
> IAM アイデンティティセンターの組織インスタンスが存在する場合は、ユースケースに IAM アイデンティティセンターの独自のアカウントインスタンスが必要であることを確認してください。存在しない場合は、[キャンセルして組織インスタンスを使用する] を選択してください。

5. オプション。このアカウントインスタンスに関連付けるタグを追加します。

コンソールに、正常にアカウントインスタンスが作成されたことが通知され、インスタンス ID が入力されます。[設定の概要] でインスタンスに名前を付けることができます。

> **Note**
>
> アカウントインスタンスでは、多要素認証 (MFA) がデフォルトで有効です。デバイス、ブラウザ、または場所が変更されると、ユーザーは MFA でサインインするように求められます。セキュリティのベストプラクティスとして、従業員の ID には MFA を強くお勧めします。IAM Identity Center で MFA デバイスを管理 についてはこちら。

ID ソースの確認、多要素認証設定の調整、 AWS マネージドアプリケーションの追加などの管理機能は、IAM Identity Center コンソールで完了する必要があります。

認証

ユーザーは自分のユーザー名を使用して AWS アクセスポータルにサインインします。その際、IAM Identity Center は、ユーザーの E メールアドレスに関連付けられたディレクトリに基づいて、IAM Identity Center 認証サービスにリクエストをリダイレクトします。認証されると、ユーザーは、追加のサインインプロンプトなしでポータルに表示されるアカウント AWS とサードパーティー software-as-a-service (SaaS) アプリケーションへのシングルサインオンアクセスが可能になります。つまり、ユーザーは、毎日使用するさまざまな割り当てられた AWS アプリケーションの複数のアカウント認証情報を追跡する必要がなくなります。

認証セッション

IAM Identity Center によって維持される認証セッションには、ユーザーの IAM Identity Center へのサインインを表す認証セッションと、Amazon SageMaker Studio や Amazon Managed Grafana などの AWS マネージドアプリケーションへのユーザーのアクセスを表す認証セッションの 2 種類があります。ユーザーが IAM アイデンティティセンターにサインインするたびに、IAM アイデンティティセンターで設定した期間 (最大 90 日間) のサインインセッションが作成されます。詳細については、「AWS アクセスポータルと IAM Identity Center 統合アプリケーションのセッション期間を管理する」を参照してください。ユーザーがアプリケーションにアクセスするたびに、IAM アイデンティティセンターサインインセッションを使用して、そのアプリケーションのアプリケーションセッションが取得されます。IAM Identity Center アプリケーションセッションの有効期間は 1 時間で、リフレッシュできます。ですので、IAM Identity Center アプリケーションセッションは、取得元の IAM Identity Center サインインセッションが有効である限り、1 時間ごとに自動的に更新されます。ユーザーが IAM Identity Center を使用して AWS Management Console または CLI にアクセスする場合、IAM Identity Center サインインセッションを使用して、対応する IAM Identity Center アクセス許可セットで指定されている IAM セッションを取得します (具体的には、IAM Identity Center は、IAM Identity Center が管理する IAM ロールをターゲットアカウントで引き受けます) 。

IAM Identity Center でユーザーを無効または削除するとすぐに、そのユーザーは新しい IAM Identity Center のサインインできなくなり、セッションが作成されません。IAM Identity Center サインインセッションは 1 時間キャッシュされます。ですので、IAM Identity Center サインインセッションがアクティブな状態でユーザーを無効にしたり削除したりしても、そのユーザーの既存の IAM Identity Center サインインセッションは、サインインセッションが最後にリフレッシュされた時間に応じて、最大 1 時間まで継続されます。この間、ユーザーは新しい IAM Identity Center アプリケーションと IAM ロールセッションを開始することができます。

IAM Identity Center サインインセッションが終了すると、ユーザーは新しい IAM Identity Center アプリケーションまたは IAM ロールセッションを開始することができなくなります。IAM アイデンティティセンターアプリケーションのセッションは、最大 1 時間までキャッシュすることができ、IAM アイデンティティセンターサインインセッションが終了した後、ユーザーはアプリケーションへのアクセスを最大 1 時間まで保持することができます。既存の IAM ロールセッションは、IAM Identity Center アクセス権限セットで設定された持続時間 (管理者が設定可能、最大 12 時間) により継続されます。

以下の表は、これらの動作をまとめたものです。

ユーザーエクスペリエンス/システム動作	ユーザーが無効化または削除されてからの時間
ユーザーが IAM Identity Center にサインインできなくなり、ユーザーが新しい IAM Identity Center サインインセッションを取得できません	なし (すぐに有効)
ユーザーが IAM Identity Center を介して新しいアプリケーションまたは IAM ロールのセッションを開始できなくなりました	最長 1 時間
ユーザーがアプリケーションにアクセスできなくなります (すべてのアプリケーションのセッションが終了します)	最大 2 時間 (IAM アイデンティティセンターサインインセッションの有効期限は最大 1 時間、IAM アイデンティティセンターアプリケーションセッションの有効期限は最大 1 時間)。
ユーザーは IAM Identity Center AWS アカウント 経由で にアクセスできなくなります	最大 13 時間 (IAM Identity Center サインインセッションの有効期限が最大 1 時間、管理者が設定した IAM ロールのセッションの有効期限がアクセス権限セットの IAM Identity Center セッションの有効期限設定に応じて最大 12 時間)。

セッションの詳細については、「セッション期間の設定」を参照してください。

ワークフォース ID の管理

AWS Identity and Access Management (IAM) は、アイデンティティと AWS サービスとリソースへのアクセスを安全に管理するのに役立ちます。AWS IAM Identity Center は IAM サービスとして、ワークフォース IDを AWS で一度に作成・接続し、複数の AWS アカウント やアプリケーショ ンへのアクセスを一元管理します。

IAM Identity Center の顧客については、複数の AWS アカウント またはアプリケーションへのアクセスを一元管理する方法に変更はありません。IAM Identity Center を初めて利用するお客様は、IAM Identity Center を使用する単一アクセス管理と並行して実行するか、IAM を使用する単一 AWS アカウント アクセス管理に取って代わるように柔軟に設定できます。

トピック

ユースケース

IAM Identity Center を使用してさまざまなビジネスニーズを満たす方法を示すユースケースを以下に示します。

トピック

AWS アプリケーションへの SSO アクセスを有効にする (アプリケーション管理者ロール)

このユースケースは、お客様が Amazon SageMaker や AWS IoT SiteWise などの AWS マネージドアプリケーション を管理するアプリケーション管理者で、ユーザーにシングルサインオンアクセスを提供する必要がある場合のガイダンスを提供します。

開始する前に、次について検討してください。

- テスト環境や本番環境を AWS Organizations で独立した組織に構築するべきでしょうか？
- IAM Identity Center は既に組織で有効になっていますか? AWS Organizations の管理アカウントで IAM Identity Center を有効にする権限がありますか？

次のガイダンスを確認して、ビジネスニーズに基づいて次のステップを決定してください。

スタンドアロンの AWS アカウント アカウントに AWS アプリケーションを設定する

AWS アプリケーションへのシングルサインオンアクセスを提供する必要があり、IT 部門がまだ IAM Identity Center を使用していない場合は、スタンドアロン AWS アカウント を作成して開始する必要があります。デフォルトでは、自分の AWS アカウント を作成すると、自分の AWS 組織の作成と管理に必要な権限が与えられます。IAM Identity Center を有効にするには、AWS アカウントのルートユーザー 権限が必要です。

IAM Identity Center と AWS Organizations は、一部の AWS アプリケーション（Amazon Managed Grafana など）のセットアップ時に自動的に有効になります。AWS アプリケーションにこれらのサービスを有効にするオプションがない場合は、アプリケーションへのシングルサインオン・アクセスを提供する前に AWS Organizations と IAM Identity Center をセットアップする必要があります。

組織では IAM Identity Center が設定されていません

アプリケーション管理者としての役割では、権限によっては IAM Identity Center を有効にできない場合があります。IAM Identity Center では、AWS Organizations 管理アカウントにおける特定の権限が必要です。この場合、適切な管理者に連絡して、組織管理アカウントで IAM アイデンティティセンターを有効にします。

IAM Identity Center を有効にするための十分な権限がある場合は、アプリケーションのセットアップを続行する前にこの操作を実行します。詳細については、「IAM アイデンティティセンターで一般的なタスクを開始する」を参照してください。

組織では IAM Identity Center が設定されていません

このシナリオでは、追加の手順や要件なしに、AWS アプリケーションのデプロイを継続することができます。

> **Note**
>
> お客様の組織が 2019 年 11 月 25 日以前に管理アカウントで IAM アイデンティティセンターを有効にした場合、管理アカウントおよびオプションでメンバーアカウントでも AWS マネージドアプリケーションを有効にする必要があります。管理アカウントだけを有効にしておけば、後からメンバーアカウントを有効にすることができます。これらのアプリケーションを有効にするには、IAM アイデンティティセンターコンソールの [設定] ページの [AWS マネージドアプリケーション] セクションで [アクセスを有効にする] を選択します。詳細については、「ID 情報を共有するための IAM アイデンティティセンターの設定」を参照してください。

Amazon EC2 Windows インスタンスへのシングルサインオン・アクセスを有効にします

Identity Center ディレクトリ（IAM Identity Center のデフォルトの ID ソース）またはサポートされている外部 ID プロバイダー（IdP）でユーザーを管理するアプリケーション管理者であり、AWS Fleet Manager コンソールから Amazon EC2 Windows デスクトップに IAM Identity Center アクセスを提供する必要がある場合、Amazon EC2 Windows インスタンスへのシングルサインオン・アクセスを有効にできます。

この設定では、既存の企業の認証情報を使用して、Amazon EC2 Windows インスタンスに安全にアクセスすることができます。管理者認証情報の共有、認証情報への複数回のアクセス、リモートアクセスクライアントソフトウェアの設定などが不要になります。Amazon EC2 Windows インスタンスへのアクセスを、複数の AWS アカウント アカウントにまたがって大規模に集中的に付与・解除することができます。例えば、従業員を IAM Identity Center 統合 ID ソースから削除すると、Amazon EC2 Windows インスタンスを含む AWS のすべてのリソースへのアクセスが自動的に失われます。

詳細については、「IAM Identity Center による Amazon EC2 Windows インスタンスへのセキュアでシームレスなシングルサインオンを実現する方法」を参照してください。

この機能を有効にするための IAM Identity Center の設定方法のデモについては、「IAM Identity Center による Amazon EC2 Windows へのシングルサインオンの実現」() を参照してください。

ユーザー、グループ、プロビジョニング

IAM アイデンティティセンターでユーザーとグループを使用する場合は、次の点に注意してください。

ユーザー名と E メールアドレスの一意性

IAM アイデンティティセンターのユーザーは一意に識別できる必要があります。IAM Identity Center では、ユーザーの主要な識別子となるユーザー名を実装しています。ほとんどの人は、ユーザー名をユーザーの E メールアドレスと同じにしていますが、IAM アイデンティティセンターと SAML 2.0 標準ではこれは必要ありません。ただ、SAML 2.0 ベースのアプリケーションの多くは、ユーザーの一意の識別子として E メールアドレスを使用しています。これらのアプリケーションは、SAML 2.0 ID プロバイダーが認証中に送信するアサーションからこの情報を取得します。このようなアプリケーションは、各ユーザーの E メールアドレスの一意性に依存します。この理由により、IAM アイデンティティセンターでは、ユーザーのサインインに E メールアドレス以外のものを指定することができます。IAM Identity Center では、ユーザーのすべてのユーザー名と E メールアドレスが、NULL ではない一意なものである必要があります。

グループ

グループは、定義するユーザーの論理的な組み合わせです。グループを作成し、グループにユーザーを追加できます。IAM Identity Center は、グループ (ネストされたグループ) へのグループの追加をサポートしていません。グループは、AWS アカウント やアプリケーションへのアクセスを割り当てる際に便利です。各ユーザーを個別に割り当てるのではなく、グループに権限を与えます。その後、グループにユーザーを追加したり削除したりすると、そのユーザーはグループに割り当てられたアカウントやアプリケーションへのアクセス権を動的に得たり、失ったりします。

ユーザーおよびグループのプロビジョニング

プロビジョニングは、ユーザーおよびグループの情報を IAM アイデンティティセンターおよび AWS マネージドアプリケーションまたはカスタマーマネージドアプリケーションで使用できるようにするプロセスです。IAM アイデンティティセンターでは、ユーザーやグループを直接作成することも、Active Directory や外部の ID プロバイダーに登録されているユーザーやグループを利用することもできます。IAM アイデンティティセンターを使用して AWS アカウント 内のユーザーとグループのアクセス許可を割り当てる前に、IAM アイデンティティセンターはまずユーザーとグループを認識する必要があります。同様に、AWS マネージドアプリケーションとカスタマーマネージドアプリケーションは、IAM アイデンティティセンターが認識しているユーザーやグループと連携することができます。

IAM Identity Center のプロビジョニングは、使用する ID ソースに応じて異なります。詳細については、「ID ソースを管理する」を参照してください。

ID ソースを管理する

IAM Identity Center の ID ソースは、ユーザーやグループがどこで管理されているかを定義します。ID ソースの設定が完了すると、ストアでユーザーまたはグループを検索して、AWS アカウント、アプリケーション、またはその両方へのシングルサインオンアクセスを付与することができます。

ID ソースは AWS Organizations で組織あたり 1 つのみ持つことができます。ID ソースとして以下のいずれかを選択できます。

- 「Identity Center ディレクトリ —」 IAM Identity Center を初めて有効にすると、デフォルトの ID ソースとして Identity Center ディレクトリで自動的に設定されます。ここでは、ユーザーとグループを作成し、AWS アカウント やアプリケーションへのアクセスレベルを割り当てることができます。
- Active Directory – AWS Directory Service を使用した AWS Managed Microsoft AD ディレクトリ、または Active Directory (AD) の自己管理ディレクトリのいずれかでユーザーの管理を継続する場合は、このオプションを選択します。
- 外部 ID プロバイダー Okta や Microsoft Entra ID などの外部 ID プロバイダー (IdP) でユーザーを管理したい場合は、このオプションを選択します。

> **Note**
>
> IAM Identity Center は SAMBA4 ベースの Simple AD をアイデンティティソースとしてサポートしていません。

トピック

ID ソースの変更に関する注意事項

アイデンティティソースはいつでも変更できますが、この変更が現在のデプロイにどのように影響するかを検討することをお勧めします。

あるアイデンティティソースですでにユーザーとグループを管理している場合、別のアイデンティティソースに変更すると、IAM Identity Center で設定したユーザーとグループの割り当てがすべて削除される可能性があります。この場合、IAM Identity Center の管理ユーザーを含むすべてのユーザーは、 AWS アカウント およびアプリケーションへのシングルサインオンアクセスを失います。

IAM Identity Center の ID ソースを変更する前に、以下の考慮事項を確認してください。ID ソースの変更を続行する場合は、詳細について アイデンティティソースを変更する を参照してください。

IAM Identity Center と Active Directory 間の切り替え

すでに Active Directory でユーザーとグループを管理している場合は、IAM Identity Center を有効にして ID ソースを選択するときに、ディレクトリの接続を検討することをお勧めします。デフォルトの Identity Center ディレクトリにユーザーやグループを作成して割り当てを行う前に、この作業を行ってください。

既に Identity Center のデフォルトディレクトリでユーザーとグループを管理している場合は、次の点を考慮してください。

- 割り当ての削除、ユーザーとグループの削除 — ID ソースを Active Directory に変更すると、ユーザーとグループが Identity Center ディレクトリから削除されます。この変更により、割り当ても削除されます。この場合、Active Directory に変更した後に、Active Directory のユーザーとグループを Identity Center ディレクトリに同期してから、それらの割り当てを再適用する必要があります。

  Active Directory を使用しない場合は、Identity Center のディレクトリにユーザーとグループを作成し、割り当てを行う必要があります。
- ID が削除されても割り当ては削除されない — Identity Center ディレクトリで ID が削除されると、IAM Identity Center でも対応する割り当てが削除されます。しかし、Active Directory では、ID が削除されても (Active Directory でも同期された ID でも)、対応する割り当ては削除されません。
- API のアウトバウンド同期なし — Active Directory をアイデンティティソースとして使用する場合、「作成、更新、および削除」API は注意して使用することをお勧めします。IAM Identity Center はアウトバウンド同期をサポートしていないため、これらの API を使用してユーザーまた

はグループに加えた変更によってアイデンティティソースが自動的に更新されることはありません。

- アクセスポータル URL が変更される – IAM Identity Center と Active Directory の間で ID ソースを変更すると、 AWS アクセスポータルの URL も変更されます。

IAM Identity Center がユーザーとグループをどのようにプロビジョニングするかについては、「Microsoft AD ディレクトリへの接続」を参照してください。

IAM Identity Center から外部 IdP への変更

ID ソースを IAM Identity Center から外部 ID プロバイダー (IdP) に変更する場合は、次の点を考慮してください。

- 割り当てとメンバーシップは正しいアサーションで機能します – ユーザー割り当て、グループ割り当て、グループメンバーシップは、新しい IdP が正しいアサーション (SAML nameIDs。これらのアサーションは、IAM Identity Center のユーザー名とグループと一致する必要があります。
- アウトバウンド同期なし – IAM Identity Center はアウトバウンド同期をサポートしていないため、IAM Identity Center で行ったユーザーとグループの変更により、外部 IdP が自動的に更新されることはありません。
- SCIM プロビジョニング – SCIM プロビジョニングを使用している場合、ID プロバイダーが IAM Identity Center に変更を送信した後でのみ、ID プロバイダーのユーザーとグループへの変更は IAM Identity Center に反映されます。自動プロビジョニングを使用する際の注意事項 を参照してください。
- ロールバック — ID ソースは、いつでも IAM Identity Center を使用して に戻すことができます。IAM Identity Center から外部 IdP への変更 を参照してください。

IAM Identity Center がユーザーとグループをどのようにプロビジョニングするかについては、「外部 ID プロバイダに接続する方法には」を参照してください。

IAM Identity Center から外部 IdP への変更

ID ソースを IAM Identity Center から外部 ID プロバイダー (IdP) に変更する場合は、次の点を考慮してください。

- IAM Identity Center センターではすべての割り当てが保持されます。

- パスワードリセットを強制する — IAM Identity Center でパスワードを持っていたユーザーは、以前のパスワードでサインインを続けることができます。外部 IdP にいて、IAM Identity Center にいなかったユーザーに対して、パスワードリセットを強制する必要があります。

IAM Identity Center がユーザーとグループをどのようにプロビジョニングするかについては、「IAM Identity Center で ID を管理する」を参照してください。

ある外部 IdP から別の外部 IdP への変更

IAM Identity Center の ID ソースとして既に外部 IdP を使用していて、別の外部 IdP に変更する場合は、次の点を考慮してください。

- アサインメントとメンバーシップは正しいアサーションで機能する – IAM Identity Center はアサインメントをすべて保持します。新しい IdP が正しいアサーション (SAML nameID など) を送信する限り、ユーザー割り当て、グループ割り当て、およびグループメンバーシップは引き続き機能します。

  これらのアサーションは、ユーザーが新しい外部 IdP を介して認証する際に、IAM Identity Center のユーザー名と一致する必要があります。
- SCIM プロビジョニング – IAM Identity Center へのプロビジョニングに SCIM を使用している場合は、SCIM を有効にしたときに新しいプロバイダーがユーザーとグループを正しくマッチさせるために、本ガイドの IdP 固有の情報や IdP のドキュメントを確認することをお勧めします。

IAM Identity Center がユーザーとグループをどのようにプロビジョニングするかについては、「外部 ID プロバイダに接続する方法には」を参照してください。

IAM Identity Center と Active Directory の切り替え

アイデンティティソースを外部 IdP から Active Directory に、または Active Directory から外部 IdP に変更する場合は、次の点を考慮してください。

- ユーザー、グループ、割り当てが削除される — すべてのユーザー、グループ、および割り当てが IAM Identity Center から削除されます。外部の IdP や Active Directory のユーザーやグループの情報は影響を受けません。
- ユーザーのプロビジョニング — 外部 IdP に変更した場合、ユーザーのプロビジョニングに IAM Identity Center を設定する必要があります。または、外部 IdP のユーザーやグループを手動でプロビジョニングしてから、割り当てを設定する必要があります。

- アサインメントとグループの作成 — Active Directory に変更する場合は、Active Directory 内のディレクトリにあるユーザーとグループを使用してアサインメントを作成する必要があります。

IAM Identity Center がユーザーとグループをどのようにプロビジョニングするかについては、「Microsoft AD ディレクトリへの接続」を参照してください。

アイデンティティソースを変更する

以下の手順では、IAM Identity Center が提供するディレクトリ (デフォルトの ID センターディレクトリ) から Active Directory または外部 ID プロバイダ、またはその逆に変更する方法について説明します。次に進む前に、ID ソースの変更に関する注意事項の情報を確認してください。現在のデプロイメントによっては、この変更により IAM Identity Center で設定したユーザーとグループの割り当てがすべて削除される可能性があります。この場合、IAM Identity Center の管理ユーザーを含むすべてのユーザーが、AWS アカウント およびアプリケーショ ンへのシングルサインオンアクセスを失います。

アイデンティティソースを変更するには

1. IAM Identity Center コンソールを開きます。
2. [Settings] (設定) を選択します。
3. [設定] ページの [ID ソース] タブを選択します。[アクション] を選択し、[ID ソースの変更] を選択します。
4. [ID ソースを変更] ページで、切り替え先のソースを選択し、[次へ] を選択します。

   Active Directory に変更する場合は、次のページのメニューから使用可能なディレクトリを選択します。

   > **Important**
   >
   > ID ソースを Active Directory に変更したり、Active Directory から変更したりすると、ID センターのディレクトリからユーザーとグループが削除されます。この変更により、IAM Identity Center で設定した割り当てもすべて削除されます。

   外部 ID プロバイダーに切り替えるには、外部 ID プロバイダに接続する方法の手順を実施することをお勧めします。
5. 免責事項を読み、次に進む準備ができたら、[許諾] と入力してください。

6. [Change identity source] (ID ソースの変更) を選択します。アイデンティティソースを Active Directory に変更する場合は、次のステップに進んでください。
7. ID ソースを Active Directory に変更すると、[設定] ページが表示されます。[設定] ページでは、次のいずれかの操作を行います。

   - [ガイド付きセットアップ] を選択します。ガイド付きセットアッププロセスを完了する方法についての詳細は、ガイド付きセットアップを参照してください。
   - [アイデンティティソース] セクションで、[アクション] を選択し、[同期の管理] を選択して、[同期範囲]、つまり同期するユーザーとグループのリストを設定します。

すべての ID ソースタイプのサインインと属性の使用を管理

IAM Identity Center には、管理者が AWS アクセスポータルの使用を制御し、 AWS アクセスポータルとアプリケーションのユーザーのセッション期間を設定し、アクセスコントロールに属性を使用できるようにする以下の一連の機能が用意されています。これらの機能は Identity Center ディレクトリまたは外部 ID プロバイダーを ID ソースとして使用します。

> **Note**
>
> Active Directory を IAM Identity Center の ID ソースとして使用している場合、セッション管理はサポートされていません。

トピック

- AWS アクセスポータルと IAM Identity Center 統合アプリケーションのセッション期間を管理する
- AWS アクセスポータルと IAM Identity Center 統合アプリケーションのセッション期間を設定する
- AWS アクセスポータルと AWS 統合アプリケーションのセッションを削除する
- サポートされているユーザーおよびグループ属性

AWS アクセスポータルと IAM Identity Center 統合アプリケーションのセッション期間を管理する

IAM Identity Center 管理者は、IAM Identity Center と と統合された両方のアプリケーションのセッション期間を設定できます AWS アクセスポータル。セッション期間の設定により、ユーザーが再認証する必要がある頻度が決まります。IAM Identity Center 管理者は、アクティブな AWS アクセス

ポータルセッションを終了し、これにより、統合されたアプリケーションのセッションを終了することもできます。

詳細については、「AWS アクセスポータルと IAM Identity Center 統合アプリケーションのセッション期間を設定する」を参照してください。およびエンドユーザーセッションの管理方法の詳細については、「」を参照してくださいAWS アクセスポータルと AWS 統合アプリケーションのセッションを削除する。

> **Note**
>
> AWS アクセスポータルのセッション期間を変更し、 AWS アクセスポータルのセッションを終了しても、アクセス許可セットで定義した AWS マネジメントコンソールのセッション期間には影響しません。

AWS アクセスポータルと IAM Identity Center 統合アプリケーションのセッション期間を設定する

AWS アクセスポータル および IAM Identity Center 統合アプリケーションへの認証のセッション期間は、ユーザーが再認証なしでサインインできる最大時間です。デフォルトのセッション期間は 8 時間です。IAM Identity Center 管理者は、15 分から最大 90 日までの異なる期間を指定できます。認証セッションの期間とユーザー動作の詳細については、「」を参照してください認証。

以下のトピックでは、 AWS アクセスポータルと IAM Identity Center 統合アプリケーションのセッション期間の設定について説明します。

トピック

- 前提条件と考慮事項
- セッション期間を設定するには

前提条件と考慮事項

AWS アクセスポータルと IAM Identity Center 統合アプリケーションのセッション期間を設定するための前提条件と考慮事項を次に示します。

外部 ID プロバイダー

IAM Identity Center は SAML アサーションの `SessionNotOnOrAfter` 属性を使用して、セッションが有効になる期間を決定します。

- `SessionNotOnOrAfter` が SAML アサーションで渡されない場合、 AWS アクセスポータルセッションの期間は、外部 IdP セッションの時間による影響を受けません。例えば、IdP セッション期間が 24 時間で、IAM Identity Center で 18 時間のセッション期間を設定した場合、ユーザーは 18 時間後に AWS アクセスポータルで再認証する必要があります。
- `SessionNotOnOrAfter` が SAML アサーションで渡された場合、セッション期間値は、 AWS アクセスポータルのセッション期間と SAML IdP セッション期間のうち短い方に設定されます。IAM Identity Center で 72 時間のセッション期間を設定し、IdP のセッション期間が 18 時間の場合、ユーザーは IdP で定義されている 18 時間の AWS リソースにアクセスできます。
- IdP のセッション時間が IAM Identity Center で設定されたセッションよりも長い場合、ユーザーは IdP との有効なログインセッションに基づいて、認証情報を再入力せずに新しい IAM Identity Center セッションを開始できます。

> **Note**
>
> Active Directory を IAM Identity Center の ID ソースとして使用している場合、セッション管理はサポートされていません。

AWS CLI および SDK セッション

AWS Command Line Interface、 AWS Software Development Kits (SDKs)、またはその他の AWS 開発ツールを使用してプログラムで AWS サービスにアクセスする場合は、 AWS アクセスポータルと IAM Identity Center 統合アプリケーションのセッション期間を設定するために、次の前提条件を満たす必要があります。

- アクセスAWS ポータルのセッション期間は、IAM Identity Center コンソールで設定する必要があります。
- 共有 AWS 設定ファイルでシングルサインオン設定用のプロファイルを定義する必要があります。このプロファイルは、 AWS アクセスポータルへの接続に使用されます。SSO トークンプロバイダーの設定を使用することをお勧めします。この設定では、 AWS SDK またはツールが更新された認証トークンを自動的に取得できます。詳細については、AWS SDK とツールリファレンスガイドの SSO トークンプロバイダーの設定 を参照してください。
- ユーザーは、セッション管理をサポートするバージョンの AWS CLI または SDK を実行する必要があります。

AWS CLI セッション管理をサポートする最小バージョン

セッション管理 AWS CLI をサポートする の最小バージョンは次のとおりです。

- AWS CLI V2 2.9 以降
- AWS CLI V1 1.27.10 以降

AWS CLI 最新バージョンをインストールまたは更新する方法については、「 の最新バージョンのインストールまたは更新 AWS CLI」を参照してください。

ユーザーが を実行している場合 AWS CLI、IAM Identity Center セッションの有効期限が切れる直前にアクセス許可セットを更新し、セッション期間を 20 時間に設定し、アクセス許可セットの期間を 12 時間に設定すると、 AWS CLI セッションは最大 20 時間 + 12 時間、合計 32 時間実行されます。IAM Identity Center CLI の使用の詳細については、AWS CLI コマンドリファレンス を参照してください。

IAM Identity Center のセッション管理をサポートする SDK の最小バージョン

IAM Identity Center のセッション管理をサポートする SDK の最小バージョンは次のとおりです。

SDK	最小バージョン
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)
Go V2	SDK 全体：リリース-2022-11-11 および特定の Go モジュール：認証情報/v1.13.0、構成/v1.18.0
JS V2	2.1253.0
JS V3	v3.210.0
C++	1.9.372

SDK	最小バージョン
.NET	v3.7.400.0

セッション期間を設定するには

AWS アクセスポータルと IAM Identity Center 統合アプリケーションのセッション期間を設定するには、次の手順に従います。

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. 「設定」 ページで、「認証」タブを選択します。
4. [認証] の [セッション設定] の横にある [設定] を選択します。[セッション設定を構成] のダイアログボックスが表示されます。
5. [セッション設定を構成] のダイアログボックスで、下矢印を選択して、ユーザーの最大セッション時間を分、時間、日単位で選択します。セッションの長さを選択し、[保存] を選択します。[設定] ページに戻ります。

AWS アクセスポータルと AWS 統合アプリケーションのセッションを削除する

IAM Identity Center ユーザーのアクティブなセッションを表示および削除するには、次の手順に従います。

AWS アクセスポータルと IAM Identity Center 統合アプリケーションのアクティブなセッションを削除するには

1. IAM Identity Center コンソール を開きます。
2. ユーザー を選択します。
3. ユーザー ページで、セッションを管理したいユーザーのユーザー名を選択します。これにより、ユーザー情報が表示されるページに移動します。
4. ユーザーのページで、「アクティブセッション」タブを選択します。「アクティブセッション」の横の括弧内の数字は、このユーザーの現在のアクティブセッション数を示します。
5. 削除する ID プロバイダーの横にあるチェックボックスを選択してから、[セッションを削除] を選択します。このユーザーのアクティブセッションを削除することを確認するダイアログボックスが表示されます。ダイアログボックスの情報を読み、続行する場合は [セッションを削除] を選択します。

6. ユーザーのページに戻ります。選択したセッションが正常に削除されたことを示す緑色のフラッシュバーが表示されます。

失効した認証セッションの動作の詳細については、「」を参照してください認証セッション。

サポートされているユーザーおよびグループ属性

属性とは、name、email、members など、個々のユーザーやグループのオブジェクトを定義し、識別するための情報のことです。IAM Identity Center は、ユーザー作成時に手動で入力された属性や、SCIM (System for Cross-Domain Identity Management) 仕様で定義されているような同期エンジンを使用して自動的にプロビジョニングされた属性に関わらず、最も一般的に使用される属性をサポートします。仕様の詳細については、https://tools.ietf.org/html/rfc7642 を参照してください。手動および自動プロビジョニングの詳細については、「ユーザーが外部の IdP から来た場合のプロビジョニング」を参照してください。

IAM Identity Center は自動プロビジョニングのユースケースのために SCIM をサポートしているので、Identity Center は、いくつかの例外を除いて、SCIM 仕様に記載されているのと同じユーザーとグループの属性をすべてサポートしています。次のセクションでは、IAM Identity Center がサポートしていない属性について説明します。

ユーザーオブジェクト

SCIM ユーザースキーマ (https://tools.ietf.org/html/rfc7643#section-8.3) のすべての属性は、IAM Identity Center ID ストアでサポートされていますが、以下を除きます。

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

ユーザーのすべてのサブ属性がサポートされていますが、以下の項目はサポートされていません。

- 複数の値を持つ属性のうち、`'display'` の副属性 (例えば、`emails` や `phoneNumbers` など)
- `'meta'` 属性の `'version'` サブ属性

オブジェクトをグループ化

SCIM グループスキーマ (https://tools.ietf.org/html/rfc7643#section-8.4) のすべての属性がサポートされています。

グループのすべてのサブ属性は、以下を除いてサポートされています。

- 多値属性 (例: メンバー) の `'display'` サブ属性。

IAM Identity Center で ID を管理する

IAM Identity Center は、ユーザーとグループに以下の機能を提供します。

- ユーザーとグループを作成します。
- ユーザーをメンバーとしてグループに追加します。
- グループには、 AWS アカウント およびアプリケーションへの必要なレベルのアクセスを割り当てます。

IAM Identity Center ストアでユーザーとグループを管理するために、 は Identity Center アクションにリストされている API オペレーション AWS をサポートします。

IAM Identity Center にいるユーザーのプロビジョニング

IAM Identity Center で直接ユーザーやグループを作成した場合、プロビジョニングは自動的に行われます。これらの ID は、割り当てを行う際や、アプリケーションで使用する際にすぐに利用できます。詳細については、「ユーザーおよびグループのプロビジョニング」を参照してください。

ID ソースの変更

でユーザーを管理する場合は AWS Managed Microsoft AD、いつでも Identity Center ディレクトリの使用を停止し、代わりに を使用して IAM Identity Center を Microsoft AD のディレクトリに接続できます AWS Directory Service。詳細については、「IAM Identity Center と Active Directory 間の切り替え」の考慮事項を参照してください。

ユーザーを外部の ID プロバイダー (IdP) で管理したい場合は、IAM Identity Center を IdP に接続し、自動プロビジョニングを有効にすることができます。詳細については、「IAM Identity Center から外部 IdP への変更」の考慮事項を参照してください。

トピック

- ユーザーの追加
- グループの追加
- グループにユーザーを追加
- IAM Identity Center でグループを削除
- IAM Identity Center でユーザーを削除する
- IAM Identity Center でユーザーアクセスを無効にする
- ユーザーのプロパティの編集
- エンドユーザーの IAM Identity Center ユーザーパスワードをリセットします。
- API から作成されたユーザーのために E メールの OTP を送信
- IAM Identity Center で ID を管理する際のパスワード要件

ユーザーの追加

Identity Center ディレクトリで作成するユーザーとグループは、IAM Identity Center でのみ使用することができます。IAM Identity Center コンソールを使用して Identity Center ディレクトリにユーザーを追加するには、以下の手順に従います。または、 AWS API オペレーションを呼び出しCreateUserてユーザーを追加することもできます。

ユーザーを追加するには

1. IAM Identity Center コンソール を開きます。
2. [ユーザー] を選択します。
3. [Add user] (ユーザーを追加) をクリックして、以下の必要な情報を入力します。

    a. Username – このユーザー名は AWS アクセスポータルにサインインするために必要であり、後で変更することはできません。1 ~ 100 文字である必要があります。

    b. パスワード — パスワードの設定手順を記載した E メールを送信するか (デフォルトのオプション)、ワンタイムパスワードを生成できます。管理ユーザーを作成していて E メールを送信する場合は、アクセスできるメールアドレスを必ず指定してください。

        i. このユーザーに、パスワードの設定手順を記載したE メールを送信します。– このオプションは、件名に「Invitation to join AWS IAM Identity Center (successor to AWS Single Sign-On)」と、Amazon Web Services から宛ての E メールをユーザーに自動的に送信します。この E メールは、会社に代わって IAM Identity Center AWS アクセスポータルにアクセスするようユーザーを招待します。

> **Note**
>
> 特定の地域では、IAM ID Center が別の AWS リージョンから Amazon Simple Email Service を使用するユーザーに E メールを送信します。E メールの送信方法については、リージョン間の呼び出し を参照してください。
> IAM Identity Center サービスで送信されるすべてのメールは、アドレス no-reply@signin.aws.com または no-reply@login.awsapps.com のいずれかから送信されます。これらの送信者メールアドレスからの E メールを受け入れ、迷惑メールやスパムとして処理しないように、メールシステムを設定することをお勧めします。

ii. このユーザーと共有できるワンタイムパスワードを生成します。– このオプションでは、E メールアドレスからユーザーに手動で送信できる AWS アクセスポータル URL とパスワードの詳細が提供されます。

c. E メールアドレス — E メールアドレスは一意である必要があります。

d. E メールアドレスを確認

e. 名 — 自動プロビジョニングを行うためには、ここに名前を入力する必要があります。詳細については、「自動プロビジョニング」を参照してください。

f. 姓 — 自動プロビジョニングを行うためには、ここに名前を入力する必要があります。

g. 表示名

> **Note**
>
> (オプション) 該当する場合は、ユーザーの Microsoft 365 不変 ID などの追加属性の値を指定して、ユーザーに特定のビジネスアプリケーションへのシングルサインオンアクセスを提供できます。

4. [次へ] を選択します。
5. 該当する場合は、ユーザーを追加するグループを 1 つ以上選択し、[次へ] を選択します。
6. 「ステップ 1: ユーザーの詳細を指定する」と「ステップ 2: ユーザーをグループに追加 (オプション)」で指定した情報を確認します。いずれかのステップで [編集] を選択し、変更を加えます。両方のステップで正しい情報が指定されていることを確認したら、[ユーザーを追加] を選択します。

グループの追加

IAM Identity Center コンソールを使用して Identity Center ディレクトリにグループを追加するには、以下の手順に従います。または、 AWS API オペレーションを呼び出しCreateGroupてグループを追加することもできます。

グループを追加するには

1. IAM Identity Center コンソール を開きます。
2. [グループ] を選択します。
3. [Create group] (グループの作成) を選択します。
4. グループ名 と 説明を入力します - オプション。説明は、グループにどのようなアクセス権限が割り当てられているか (または割り当てられるか) に関する詳細を記載する必要があります。「ユーザーをグループに追加 - オプション」で、メンバーとして追加するユーザーを見つけます。それぞれの横にあるチェックボックスをオンにします。
5. [グループを作成] を選択します。

このグループを Identity Center ディレクトリに追加すると、このグループにシングルサインオンアクセスを割り当てることができます。詳細については、「へのユーザーアクセスを割り当てる AWS アカウント」を参照してください。

グループにユーザーを追加

IAM Identity Center コンソールを使用して、Identity Center ディレクトリに以前に作成したグループのメンバーとしてユーザーを追加するには、次の手順を実行します。または、 AWS API オペレーションを呼び出しCreateGroupMembershipて、ユーザーをグループのメンバーとして追加することもできます。

グループのメンバーとしてユーザーを追加するには

1. IAM Identity Center コンソール を開きます。
2. [グループ] を選択します。
3. 更新する グループ名 を選択します。
4. グループ詳細ページの「このグループのユーザー」で、「ユーザーをグループに追加」を選択します。
5. [グループにユーザーを追加] ページの [その他のユーザー] で、メンバーとして追加するユーザーを見つけます。それぞれの横にあるチェックボックスをオンにします。

6. [ユーザーの追加] を選択します。

IAM Identity Center でグループを削除

IAM アイデンティティセンターディレクトリ内のグループを削除すると、そのグループのメンバーであるすべてのユーザーの AWS アカウント および アプリケーションへのアクセス権が削除されます。グループが削除された後、元に戻すことはできません。IAM Identity Center コンソールを使用して Identity Center ディレクトリ内のグループを削除するには、以下の手順に従います。

IAM Identity Center でグループを削除するには

> **Important**
>
> このページの説明は、AWS IAM Identity Center に適用されます。これらは AWS Identity and Access Management (IAM) には適用されません。IAM Identity Center ユーザー、グループ、およびユーザー認証情報は、IAM ユーザー、グループ、IAM ユーザー認証情報とは異なります。IAM でグループを削除する手順をお探しの場合は、AWS Identity and Access Management ユーザーガイドの「IAM ユーザーグループの削除」を参照してください。

1. IAM Identity Center コンソール を開きます。
2. [グループ] を選択します。
3. グループを削除するには 2 つの方法があります。
   - グループ ページでは、複数のグループを選択して削除することができます。削除するグループ名を選択し、[グループの削除] を選択します。
   - 削除するグループ名を選択します。グループの詳細ページで、[グループの削除] を選択します。
4. グループを削除するかどうかの確認を求められる場合があります。
   - 複数のグループを一度に削除する場合は、「グループの削除」ダイアログボックスに **`Delete`** を入力して削除を確定します。
   - ユーザーを含む 1 つのグループを削除する場合は、削除するグループの名前を [グループの削除] ダイアログボックスに入力して削除を確定します。
5. [Delete group (グループの削除)] を選択します。削除するグループを複数選択した場合は、「# グループを削除」を選択します。

IAM Identity Center でユーザーを削除する

IAM アイデンティティセンターディレクトリ内のユーザーを削除すると、 AWS アカウント およびアプリケーションへのアクセスが削除されます。ユーザーが削除された後、元に戻すことはできません。IAM Identity Center コンソールを使用して Identity Center ディレクトリのユーザーを削除するには、以下の手順に従います。

> **Note**
>
> ユーザーアクセスを無効にしたり、IAM Identity Center でユーザーを削除すると、そのユーザーはすぐに AWS アクセスポータルにサインインできなくなり、新しいサインインセッションを作成できなくなります。詳細については、「認証セッション」を参照してください。

IAM Identity Center でユーザーを削除するには

> **Important**
>
> このページの説明は、AWS IAM Identity Center に適用されます。これらは AWS Identity and Access Management (IAM) には適用されません。IAM Identity Center ユーザー、グループ、およびユーザー認証情報は、IAM ユーザー、グループ、IAM ユーザー認証情報とは異なります。IAM でユーザーを削除する手順をお探しの場合は、AWS Identity and Access Management ユーザーガイドの「IAM ユーザーの削除」を参照してください。

1. IAM Identity Center コンソール を開きます。
2. [ユーザー] を選択します。
3. ユーザーを削除するには 2 つの方法があります。
   - ユーザー ページでは、削除するユーザーを複数選択できます。削除するユーザー名を選択し、[ユーザーの削除] を選択します。
   - 削除するユーザー名を選択します。ユーザーの詳細ページで、[ユーザーの削除] を選択します。
4. 複数のユーザーを一度に削除する場合は、「ユーザーの削除」 ダイアログボックスに **`Delete`** を入力して削除を確定します。

5. [ユーザーの削除] を選択します。削除するユーザーを複数選択した場合は、「#ユーザーを削除」を選択します。

IAM Identity Center でユーザーアクセスを無効にする

IAM Identity Center ディレクトリでユーザーアクセスを無効にすると、ユーザーの詳細の編集、パスワードのリセット、グループへのユーザーの追加、グループ メンバーシップの表示ができなくなります。以下の手順に従って、IAM Identity Center コンソールを使用して Identity Center ディレクトリのユーザーアクセスを無効にします。

> **Note**
>
> ユーザーアクセスを無効にしたり、IAM Identity Center でユーザーを削除すると、そのユーザーはすぐに AWS アクセスポータルにサインインできなくなり、新しいサインインセッションを作成できなくなります。詳細については、「認証セッション」を参照してください。

IAM Identity Center でユーザーアクセスを無効にするには

1. IAM Identity Center コンソール を開きます。

   > **Important**
   >
   > このページの説明は、AWS IAM Identity Center に適用されます。これらは AWS Identity and Access Management (IAM) には適用されません。IAM Identity Center ユーザー、グループ、およびユーザー認証情報は、IAM ユーザー、グループ、IAM ユーザー認証情報とは異なります。IAM でユーザーを非アクティブ化する手順をお探しの場合は、AWS Identity and Access Management ユーザーガイドの「IAM ユーザーの管理」を参照してください。

2. [ユーザー] を選択します。
3. アクセスを無効にするユーザーのユーザー名を選択します。
4. アクセスを無効にするユーザーのユーザー名の下で、「一般情報」セクションで「ユーザーアクセスを無効にする」を選択します。
5. [ユーザーアクセスの無効化] のダイアログボックスで、[ユーザーアクセスの無効化] を選択します。

ユーザーのプロパティの編集

IAM Identity Center コンソールを使用して Identity Center ディレクトリ内のユーザーのプロパティを編集するには、次の手順を実行します。または、 AWS API オペレーションを呼び出しUpdateUserてユーザープロパティを更新することもできます。

IAM Identity Center でユーザープロパティを編集するには

1. IAM Identity Center コンソール を開きます。
2. [ユーザー] を選択します。
3. 編集するユーザーを選択します。
4. ユーザー [プロファイル] ページで、[プロファイルの詳細] の横にある [編集] を選択します。
5. [プロファイル詳細の編集] ページで、必要に応じてプロパティを更新します。次に、[変更の保存] を選択します。

> **Note**
>
> (オプション) 従業員番号 や Office 365 不変 ID などの追加の属性を変更して、IAM Identity Center 内のユーザーの ID をユーザーが使用する必要がある特定のビジネスアプリケーションにマップするのに役立ちます。

> **Note**
>
> E メールアドレス属性は編集可能なフィールドで、指定する値は一意である必要があります。

エンドユーザーの IAM Identity Center ユーザーパスワードをリセットします。

この手順は IAM Identity Center ディレクトリでユーザーのパスワードをリセットする必要がある管理者を対象としています。IAM Identity Center コンソールを使用してパスワードをリセットします。

ID プロバイダーとユーザータイプに関する考慮事項

- MicrosoftActive Directory または外部プロバイダー — IAM ID Center を Microsoft Active Directory または外部プロバイダーに接続する場合、ユーザーパスワードのリセットは Active Directory 内

または外部プロバイダー内から行う必要があります。つまり、これらのユーザーのパスワードを IAM Identity Center コンソールからリセットすることはできません。

- IAM ID センターディレクトリ内のユーザー — IAM Identity Center のユーザーであれば、自分の IAM Identity Center のパスワードをリセットできます。「IAM Identity Center でユーザーのパスワードをリセットする手順」を参照してください。

IAM Identity Center のエンドユーザーのパスワードをリセットするには

> **Important**
>
> このページの説明は、AWS IAM Identity Center に適用されます。これらは AWS Identity and Access Management (IAM) には適用されません。IAM Identity Center ユーザー、グループ、およびユーザー認証情報は、IAM ユーザー、グループ、IAM ユーザー認証情報とは異なります。IAM ユーザーのパスワードを変更する手順をお探しの場合は、AWS Identity and Access Management ユーザーガイドの「IAM ユーザーのパスワードの管理」を参照してください。

1. IAM Identity Center コンソール を開きます。
2. [ユーザー] を選択します。
3. パスワードをリセットするユーザーのユーザー名を選択します。
4. ユーザーの詳細ページで、[パスワードのリセット] を選択します。
5. [Reset password] (パスワードのリセット) ダイアログボックスで、次の選択肢のいずれかを選び、[Reset password] (パスワードのリセット) を選択します。

   a. Send an email to the user with instructions to reset the password (パスワードのリセット手順が記載された E メールをユーザーに送信する) – このオプションでは、Amazon ウェブサービスから、パスワードをリセットする方法について説明する E メールアドレスを自動的にユーザーに送信します。

   > **Warning**
   >
   > セキュリティ上のベストプラクティスとして、このオプションを選択する前に、このユーザーの E メールアドレスが正しいかどうかを確認してください。このパスワードリセット E メールが誤って送信された、または誤って設定された E メールアドレスに送信された場合、悪意のある受信者がそれを使用して AWS 環境への不正アクセスを行う可能性があります。

b. ワンタイムパスワードを生成し、ユーザーと共有します – このオプションでは、E メールアドレスから手動でユーザーに送信できる、パスワードの詳細が利用できます。

API から作成されたユーザーのために E メールの OTP を送信

CreateUserAPI オペレーションを使用してユーザーを作成する場合、そのユーザーにはパスワードがありません。これを変更するには、API を使用してユーザーを作成したときに E メールワンタイムパスワード (OTP) をユーザーに送信するように選択してください。ユーザーが初めてログインしようとしたときに E メール OTP が届きます。E メール OTP を受信したユーザーは、ログイン時に新しいパスワードを設定する必要があります。この設定を有効にしない場合は、CreateUser API を使用して作成したユーザーと OTP を生成して共有する必要があります。

CreateUser API で作成されたユーザーに E メール OTP を送信するには

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. 「設定」 ページで、「認証」タブを選択します。
4. [標準認証] セクションで、[設定] を選択します。
5. ダイアログボックスが表示されます。[E メールの OTP を送信] の横にあるボックスにチェックを入れます。次に、保存を選択します。ステータスが [無効] から [有効] に更新されます。

IAM Identity Center で ID を管理する際のパスワード要件

> **Note**
>
> これらの要件は、Identity Center ディレクトリで作成されたユーザーにのみ適用されます。IAM Identity Center 以外の ID ソースを Active Directoryや外部 ID プロバイダー などの認証用に設定している場合、ユーザーのパスワードポリシーは IAM Identity Center ではなく、それらのシステムで定義され、適用されます。ID ソースが の場合 AWS Managed Microsoft AD、詳細については「 のパスワードポリシーの管理 AWS Managed Microsoft AD」を参照してください。

IAM Identity Center を ID ソースとして使用する場合、ユーザーは以下のパスワード要件を守ってパスワードを設定・変更する必要があります。

- パスワードでは、大文字と小文字が区別されます。

- パスワードの長さは8文字から64文字の間でなければなりません。
- パスワードには、次の 4 つカテゴリから少なくとも 1 文字を含める必要があります。
  - 小文字 a〜z
  - 大文字 A〜Z
  - 数字 (0〜9)
  - 英数字以外の文字 (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
- 最後の3つのパスワードは再使用できません。
- 第三者から漏洩したデータセットを通じて公に知られているパスワードは使用できません。

Microsoft AD ディレクトリへの接続

では AWS IAM Identity Center、 AWS Managed Microsoft AD を使用して Active Directory (AD) のセルフマネージドディレクトリまたは のディレクトリを接続できます AWS Directory Service。この Microsoft AD ディレクトリでは、管理者が IAM Identity Center コンソールを使用してシングルサインオンアクセスを割り当てるときに、プル元の ID プールを定義します。社内ディレクトリを IAM Identity Center に接続したら、AD ユーザーまたはグループに AWS アカウント、アプリケーション、またはその両方へのアクセス権を付与できます。

AWS Directory Service は、 AWS クラウドでホストされているスタンドアロン AWS Managed Microsoft AD ディレクトリをセットアップして実行するのに役立ちます。 AWS Directory Service を使用して、 AWS リソースを既存のセルフマネージド AD に接続することもできます。セルフマネージド AD と連携 AWS Directory Service するように を設定するには、まず信頼関係を設定して認証をクラウドに拡張する必要があります。

IAM Identity Center は、 が提供する接続 AWS Directory Service を使用して、ソース AD インスタンスへのパススルー認証を実行します。を ID ソース AWS Managed Microsoft AD として使用すると、IAM Identity Center は AD 信頼を介して接続された任意のドメインから、 AWS Managed Microsoft AD または任意のドメインからユーザーと連携できます。4 つ以上のドメインにユーザーを配置したい場合、ユーザーは IAM Identity Center へのサインインを実行する際に、ユーザー名として `DOMAIN\user` 構文を使用する必要があります。

> **メモ**
>
> - 前提条件のステップとして、 AWS Managed Microsoft AD の AD Connector または ディレクトリが AWS Organizations 管理アカウント内 AWS Directory Service に存在することを

確認します。詳細については、「IAM Identity Center で ID ソースを確認する」を参照してください。

- IAM Identity Center は、SAMBA4 ベースの Simple AD を接続先ディレクトリとしてサポートしていません。

Active Directory を使用する際の考慮事項

Active Directory を ID ソースとして使用する場合、設定は次の前提条件を満たす必要があります。

- を使用している場合は AWS Managed Microsoft AD、 AWS Managed Microsoft AD ディレクトリがセットアップされている AWS リージョン のと同じ で IAM Identity Center を有効にする必要があります。IAM Identity Center では、割り当てデータに関するディレクトリと同じリージョンに保存されます。IAM Identity Center を管理するには、IAM Identity Center が設定されているリージョンに切り替える必要がある場合があります。また、 AWS アクセスポータルは ディレクトリと同じアクセス URL を使用することに注意してください。
- 管理アカウントにある Active Directory を使用してください。

  に既存の AD Connector または AWS Managed Microsoft AD ディレクトリを設定し AWS Directory Service、 AWS Organizations 管理アカウント内に存在する必要があります。 AWS Managed Microsoft AD 一度に接続できる AD Connector ディレクトリは 1 つまたは 1 つのディレクトリのみです。複数のドメインやフォレストをサポートする必要がある場合は、 AWS Managed Microsoft ADを使用してください。詳細については、以下を参照してください。

  - のディレクトリを IAM Identity Center AWS Managed Microsoft AD に接続する
  - Active Directory の自己管理型ディレクトリを IAM Identity Center に接続する
- 委任された管理者アカウントにある Active Directory を使用してください。

  IAM Identity Center の委任された管理者を有効にし、Active Directory を IAM Identity Center のアイデンティティソースとして使用する場合は、委任された管理者アカウントにある AWS ディレクトリに設定された既存の AD Connector または AWS Managed Microsoft AD ディレクトリを使用できます。

  IAM Identity Center ID ソースを他のソースから Active Directory に変更するか、Active Directory から他のソースに変更する場合、そのディレクトリは IAM Identity Center 委任管理者メンバーアカウント (存在する場合) に存在する (所有されている) 必要があります。それ以外の場合は、管理アカウントに含まれている必要があります。

Active Directory に接続してユーザーを指定する

すでに Active Directory を使用している場合は、以下のトピックがディレクトリを IAM アイデンティティセンターに接続する準備に役立ちます。

IAM Identity Center を使用して、Active Directory の ディレクトリ AWS Managed Microsoft AD またはセルフマネージドディレクトリを接続できます。Active Directory で AWS Managed Microsoft AD ディレクトリまたはセルフマネージドディレクトリを接続する場合は、Active Directory の設定が の前提条件を満たしていることを確認してくださいIAM Identity Center で ID ソースを確認する。

> **Note**
>
> セキュリティのベストプラクティスとして、多要素認証を有効にすることを強くお勧めします。Active Directory の AWS Managed Microsoft AD ディレクトリまたはセルフマネージドディレクトリを接続する予定で、 で RADIUS MFA を使用していない場合は AWS Directory Service、IAM Identity Center で MFA を有効にします。

AWS Managed Microsoft AD

1. Microsoft AD ディレクトリへの接続 のガイダンスを確認してください。
2. 「のディレクトリを IAM Identity Center AWS Managed Microsoft AD に接続する」の手順を実行します。
3. 管理者権限を付与したいユーザーを IAM Identity Center と同期するように Active Directory を設定します。詳細については、「管理ユーザーを IAM Identity Center と同期する」を参照してください。

Active Directory 内の自己管理型ディレクトリ

1. Microsoft AD ディレクトリへの接続 のガイダンスを確認してください。
2. 「Active Directory の自己管理型ディレクトリを IAM Identity Center に接続する」の手順を実行します。
3. 管理者権限を付与したいユーザーを IAM Identity Center と同期するように Active Directory を設定します。詳細については、「管理ユーザーを IAM Identity Center と同期する」を参照してください。

外部 IdP

1. 外部 ID プロバイダに接続する方法には のガイダンスを確認してください。
2. 「外部 ID プロバイダに接続する方法」の手順を実行します。
3. IAM Identity Center にユーザーをプロビジョニングするように IdP を設定します。

> **Note**
>
> IdP から IAM Identity Center へのすべてのワークフォース ID のグループベースの自動プロビジョニングを設定する前に、管理権限を付与したい 1 人のユーザーを IAM Identity Center に同期することをお勧めします。

管理ユーザーを IAM Identity Center と同期する

ディレクトリを IAM Identity Center に接続したら、管理権限を付与するユーザーを指定し、そのユーザーをディレクトリから IAM Identity Center に同期できます。

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. 「設定」ページで「ID ソース」タブを選択し、「アクション」を選択し、「同期を管理」を選択します。
4. [同期の管理] ページで、[ユーザー] タブを選択し、[ユーザーとグループの追加] を選択します。
5. [ユーザー] タブの [ユーザー] に正確なユーザー名を入力し、[追加] を選択します。
6. [追加されたユーザーとグループ] で、次の操作を行います。
   a. 管理者権限を付与するユーザーが指定されていることを確認します。
   b. ユーザー名の左側にあるチェックボックスをオンにします。
   c. [送信] を選択します。
7. [同期の管理] ページで、指定したユーザーが同期対象のユーザーリストに表示されます。
8. ナビゲーションペインで [Users (ユーザー)] を選択します。
9. 「ユーザー」ページでは、指定したユーザーがリストに表示されるまでに時間がかかる場合があります。ユーザーリストを更新するには、[更新] アイコンをクリックします。

この時点では、ユーザーは管理アカウントにアクセスできません。このアカウントへの管理アクセスを設定するには、管理アクセス権限セットを作成し、そのアクセス権限セットにユーザを割り当てます。詳細については、「アクセス権限セットを作成します。」を参照してください。

ユーザーがアクティブディレクトリから来たときのプロビジョニング

IAM Identity Center は、 が提供する接続 AWS Directory Service を使用して、Active Directory のソースディレクトリから IAM Identity Center ID ストアにユーザー、グループ、メンバーシップ情報を同期します。ユーザー認証は Active Directory のソースディレクトリから直接行われるため、パスワード情報は IAM アイデンティティセンターに同期されません。この ID データは、アプリケーションによって使用され、LDAP アクティビティを Active Directory のソースディレクトリに戻すことなく、アプリ内検索、承認、コラボレーション シナリオを容易にします。

上記のプロビジョニングの詳細については、「ユーザーおよびグループのプロビジョニング」を参照してください。

トピック

- のディレクトリを IAM Identity Center AWS Managed Microsoft AD に接続する
- Active Directory の自己管理型ディレクトリを IAM Identity Center に接続する
- AWS Managed Microsoft AD　ディレクトリの属性マッピング
- Active Directory からユーザーとグループをプロビジョニングする

のディレクトリを IAM Identity Center AWS Managed Microsoft AD に接続する

によって管理 AWS Managed Microsoft AD される のディレクトリを IAM Identity Center に接続するには AWS Directory Service 、以下の手順に従います。

IAM Identity Center AWS Managed Microsoft AD に接続するには

1. IAM Identity Center コンソール を開きます。

   > **Note**
   >
   > 次のステップに進む前に、IAM Identity Center コンソールで、 AWS Managed Microsoft AD ディレクトリが存在するリージョンの 1 つを使用していることを確認してください。

2. [設定] を選択します。
3. [設定] ページで [ID ソース] タブを選択し、[アクション] > [ID ソースを変更]を選択します。
4. [ID ソースの選択] で [Active Directory] を選択し、[次へ] を選択します。

5. [アクティブディレクトリに接続] で、一覧から AWS Managed Microsoft AD のディレクトリを選択し、[次へ] を選択します。
6. [変更の確認] で情報を確認し、準備ができたら ACCEPT と入力し、[ID ソースを変更] を選択します。

> **Important**
>
> Active Directory 内のユーザーを IAM アイデンティティセンターの管理者ユーザーとして指定するには、まず Active Directory から管理権限を付与したいユーザーを IAM ID センターに同期する必要があります。これを行うには、「管理ユーザーを IAM Identity Center と同期する」の手順を実行します。

Active Directory の自己管理型ディレクトリを IAM Identity Center に接続する

Active Directory (AD) のセルフマネージドディレクトリのユーザーは、 AWS アクセスポータルの AWS アカウント およびアプリケーションへのシングルサインオンアクセスを持つこともできます。これらのユーザーのシングルサインオンアクセスを設定するには、次のいずれかを実行します。

- 双方向の信頼関係を作成する — と AD の自己管理型ディレクトリの間に双方向の信頼関係を作成する AWS Managed Microsoft AD と、AD の自己管理型ディレクトリのユーザーは、さまざまな AWS サービスやビジネスアプリケーションに企業の認証情報を使用してサインインできます。一方向の信頼は IAM Identity Center では機能しません。

  AWS IAM Identity Center では、ユーザーとグループのメタデータを同期するためにドメインからユーザーとグループの情報を読み取るアクセス許可を持つように、双方向の信頼が必要です。IAM Identity Center は、アクセス権限セットまたはアプリケーションへのアクセスを割り当てるときに、このメタデータを使用します。ユーザーおよびグループのメタデータは、ダッシュボードを別のユーザーやグループと共有する場合など、コラボレーションのためにアプリケーションによっても使用されます。 AWS Directory Service for Microsoft Active Directory からドメインへの信頼により、IAM Identity Center は認証のためにドメインを信頼できます。逆方向の信頼は、ユーザーおよびグループのメタデータを読み取るアクセス AWS 許可を付与します。

  双方向の信頼関係の設定の詳細については、「AWS Directory Service 管理者ガイド」の「信頼関係を作成する場合」 を参照してください。
- AD Connector を作成する - AD Connector は、クラウドに情報をキャッシュすることなく、セルフマネージドの AD にディレクトリリクエストをリダイレクトできるディレクトリゲートウェイで

す。詳細については、「AWS Directory Service 管理ガイド」の [ディレクトリへの接続]を参照してください。

> **Note**
>
> IAM Identity Center を AD Connector ディレクトリに接続している場合、今後のユーザーパスワードのリセットは、AD 内から行う必要があります。つまり、ユーザーは AWS アクセスポータルからパスワードをリセットできません。
> AD Connector を使用してアクティブディレクトリドメインサービスを IAM Identity Center に接続する場合、IAM Identity Center は AD Connector がアタッチされている単一ドメインのユーザーとグループにしかアクセスできません。複数のドメインやフォレストをサポートする必要がある場合は、Microsoft Active Directory の AWS Directory Service をご利用ください。

> **Note**
>
> IAM Identity Center は SAMBA4 ベースの Simple AD ディレクトリでは機能しません。

AWS Managed Microsoft AD ディレクトリの属性マッピング

属性マッピングは、IAM Identity Center に存在する属性タイプを、 AWS Managed Microsoft AD ディレクトリ内の同様の属性にマッピングするために使用されます。IAM Identity Center は、Microsoft AD ディレクトリのユーザー属性を検索し、IAM Identity Center のユーザー属性にマップします。IAM アイデンティティセンターのこれらのユーザー属性マッピングは、アプリケーションの SAML 2.0 アサーションを生成するためにも使用されます。アプリケーションによって、正常なシングルサインオンに必要な SAML 2.0 属性のリストは異なります。

IAM Identity Center は、アプリケーションの設定ページの [属性マッピング] タブから一連の属性を事前に取得します。IAM アイデンティティセンターは、これらのユーザー属性を使用して、アプリケーションに送信される SAML アサーション (SAML 属性) を設定します。次に、これらのユーザー属性が Microsoft AD ディレクトリから取得されます。詳細については、「アプリケーションの属性を IAM Identity Center の属性にマップする」を参照してください。

IAM Identity Center は、ディレクトリの設定ページの [属性マッピング] セクションにある一連の属性も管理します。詳細については、「IAM Identity Center の属性を AWS Managed Microsoft AD ディレクトリの属性にマッピングする」を参照してください。

サポートされているディレクトリの属性

次の表は、サポートされているディレクトリ属性と、IAM Identity Center のユーザー属性にマッピングできる AWS Managed Microsoft AD ディレクトリ属性の一覧です。

Microsoft AD ディレクトリでサポートされている属性
`${dir:email}`
`${dir:displayname}`
`${dir:distinguishedName}`
`${dir:firstname}`
`${dir:guid}`
`${dir:initials}`
`${dir:lastname}`
`${dir:proxyAddresses}`
`${dir:proxyAddresses:smtp}`
`${dir:proxyAddresses:SMTP}`
`${dir:windowsUpn}`

サポートされている Microsoft AD ディレクトリの属性の任意の組み合わせを指定して、IAM Identity Center の 1 つの変更可能な属性にマップできます。例えば、 IAM Identity Center のユーザー属性 列で `subject` 属性を選択することができます。そして、それを `${dir:displayname}`、`${dir:lastname}${dir:firstname }`、サポートされている単一の属性、またはサポートされている属性の任意の組み合わせにマッピングします。IAM Identity Center のユーザー属性のデフォルトマッピングのリストは、「デフォルトのマッピング」を参照してください。

> **Warning**
>
> IAM Identity Center の特定の属性は変更不可で、デフォルトで特定の Microsoft AD ディレクトリ属性にマップされるため、変更できません。
> 例えば、「username」は IAM Identity Center の必須属性です。「username」を空の値を持つ AD ディレクトリ属性にマッピングすると、IAM Identity Center はその`windowsUpn`値を「username」のデフォルト値と見なします。現在のマッピングから「username」の属性マッピングを変更する場合は、「username」に依存する IAM Identity Center フローが引き続き期待どおりに動作することを確認してから変更を行ってください。

ListUsers または ListGroups API アクション、または list-usersおよび list-groups AWS CLI コマンドを使用して、ユーザーおよびグループアクセスをアプリケーション AWS アカウント に割り当てる場合は、 の値を FQDN `AttributeValue`として指定する必要があります。この値は user@example.com の形式である必要があります。次の例では、`AttributeValue` が `janedoe@example.com` に設定されています。

```
aws identitystore list-users --identity-store-id d-12345a678b --filters
 AttributePath=UserName,AttributeValue=janedoe@example.com
```

サポートされている IAM Identity Center 属性

次の表は、サポートされているすべての IAM Identity Center 属性と、 AWS Managed Microsoft AD ディレクトリ内のユーザー属性にマッピングできるすべての IAM Identity Center 属性の一覧です。後で、アプリケーションの属性マッピングを設定するときに、これらの同じ IAM Identity Center の属性を、そのアプリケーションで使用されている実際の属性にマップできます。

IAM Identity Center でサポートされる属性
`${user:AD_GUID}`
`${user:email}`
`${user:familyName}`
`${user:givenName}`
`${user:middleName}`

IAM Identity Center でサポートされる属性
${user:name}
${user:preferredUsername}
${user:subject}

サポートされている外部 ID プロバイダ属性

以下の表では、サポートされているすべての外部 ID プロバイダー(IdP) 属性と、IAM Identity Center で アクセスコントロールの属性 を構成するときに使用できる属性にマッピングできるものをリストアップしたものです。SAML アサーションを使用する場合、IdP がサポートするすべて属性を使用できます。

IdP でサポートされている属性
${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}

IdP でサポートされている属性
${path:phoneNumbers[type eq "work"].value}
${path:userType}
${path:title}
${path:locale}
${path:timezone}
${path:enterprise.employeeNumber}
${path:enterprise.costCenter}
${path:enterprise.organization}
${path:enterprise.division}
${path:enterprise.department}
${path:enterprise.manager.value}

デフォルトのマッピング

次の表は、IAM Identity Center のユーザー属性と AWS Managed Microsoft AD ディレクトリのユーザー属性のデフォルトマッピングを示しています。IAM ID センターは IAM Identity Center のユーザー属性 列の属性リストのみをサポートします。

> **Note**
>
> 設定可能な AD 同期を有効にしたときに IAM Identity Center のユーザーとグループに何も割り当てられていない場合は、次の表のデフォルトマッピングが使用されます。これらのマッピングをカスタマイズする方法については、「同期の属性マッピングを設定する」を参照してください。

IAM Identity Center のユーザー属性	Microsoft AD ディレクトリのこの属性へのマップ
AD_GUID	${dir:guid}
email *	${dir:windowsUpn}
familyName	${dir:lastname}
givenName	${dir:firstname}
middleName	${dir:initials}
name	${dir:displayname}
preferredUsername	${dir:displayname}
subject	${dir:windowsUpn}

* IAM Identity Center の E メール属性はディレクトリ内で一意である必要があります。または、JIT ログインプロセスが失敗する可能性があります。

必要に応じて、デフォルトのマッピングを変更したり、SAML 2.0 アサーションに属性を追加したりできます。例えば、アプリケーションでは、User.Email SAML 2.0 属性にユーザーの E メールを要求するとします。また、E メールアドレスは、Microsoft AD ディレクトリの windowsUpn 属性に保存されていると仮定します。このマッピングのためには、IAM Identity Center コンソールで以下の 2 つの場所を変更する必要があります。

1. [Directory] (ディレクトリ) ページ、[Attribute mappings] (属性マッピング) セクションで、ユーザー属性 **email** を **${dir:windowsUpn}** 属性にマッピングする必要があります ([Maps to this attribute in your directory] (ディレクトリにあるこの属性にマップする) 列)。
2. [Applications] (アプリケーション) ページで、テーブルからアプリケーションを選択します。[Attribute mappings] (属性マッピング) タブを選択します。次に、User.Email 属性を **${user:email}** 属性にマッピングします (IAM Identity Center 列のこの文字列値またはユーザー属性にマップされる)。

ディレクトリの各属性は ${dir:**AttributeName**} 形式で指定する必要があります。例えば、Microsoft AD ディレクトリの firstname 属性は ${dir:firstname} になります。ディレク

トリのすべての属性に実際の値が割り当てられていることが重要です。属性で `${dir:` の後に値がないと、ユーザーのサインイン時に問題が発生します。

IAM Identity Center の属性を AWS Managed Microsoft AD ディレクトリの属性にマッピングする

IAM Identity Center のユーザー属性を Microsoft AD ディレクトリの対応する属性にマップする方法を指定するには、以下の手順を実行します。

IAM Identity Center の属性をディレクトリの属性にマップするには

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. [設定] ページで [アクセス制御用の属性] タブを選択し、[属性の管理] を選択します。
4. [アクセスコントロールの属性の管理] ページで、マップする IAM Identity Center の属性を見つけて、テキスト ボックスに値を入力します。例えば、IAM Identity Center ユーザー属性 **`email`** を Microsoft AD ディレクトリ属性 **`${dir:windowsUpn}`** にマップするとします。
5. [変更の保存] を選択します。

Active Directory からユーザーとグループをプロビジョニングする

IAM Identity Center では、Active Directory からユーザーとグループをプロビジョニングする次の 2 つの方法が用意されています。

- IAM Identity Center の設定可能な Active Directory (AD) 同期 (推奨) — この同期方法では、次のことが可能になります。
  - IAM Identity Center に自動的に同期される Microsoft Active Directory 内のユーザーとグループを明示的に定義することにより、データの境界を制御します。ユーザーとグループを追加 したり、ユーザーやグループを削除 したりして、同期の範囲をいつでも変更できます。
  - 同期されたユーザーとグループに、 AWS アカウントへの アプリケーションへのシングルサインオン アクセス またはアプリケーションへのアクセス権を割り当てます。アプリケーションは、 AWS マネージドアプリケーションまたはカスタマーマネージドアプリケーションです。
  - 必要に応じて同期を 一時停止したり再開 したりして、同期プロセスを制御します。これにより、実稼働システムの負荷を調整できます。
- IAM ID センター AD 同期 — この同期方法では、IAM Identity Center を使用して Active Directory 内のユーザーとグループに AWS ア カウントとアプリケーションへのアクセス権を割り当てます。割り当てられた ID はすべて IAM Identity Center に自動的に同期されます。

IAM Identity Center の構成可能な AD 同期

IAM Identity Center の設定可能な Active Directory (AD) 同期を使用すると、IAM Identity Center に自動的に同期される Microsoft Active Directory の ID を明示的に設定し、同期プロセスを制御できます。

以下のトピックでは、設定可能な AD Sync を設定および管理するための情報を提供します。

トピック

前提条件と考慮事項

設定可能な AD Sync を使用する前に、以下の前提条件と考慮事項に注意してください。

- Active Directory 内のユーザーとグループを指定して同期する

  IAM Identity Center を使用して新しいユーザーとグループに AWS マネージドアプリケーションまたはカスタマーマネージドアプリケーションへのアクセス権 AWS アカウント を割り当てる前に、同期する Active Directory のユーザーとグループを指定してから IAM Identity Center に同期する必要があります。

  - AD 同期 — IAM Identity Center コンソールまたは関連する割り当て API アクションを使用して新しいユーザーやグループに割り当てを行うと、IAM Identity Center は指定されたユーザーまたはグループをドメインコントローラーで直接検索して割り当てを完了し、ユーザーまたはグループのメタデータを IAM Identity Center に定期的に同期します。
  - 設定可能な AD 同期 — IAM Identity Center はドメインコントローラーでユーザーやグループを直接検索しません。代わりに、同期するユーザーとグループのリストを最初に指定する必要があります。IAM Identity Center に既に同期されているユーザーとグループがあるか、設定可能な AD Sync を使用して初めて同期する新しいユーザーとグループがあるかに応じて、このリスト (同期スコープとも呼ばれる) を以下のいずれかの方法で設定できます。
    - 既存のユーザーとグループ:すでに IAM Identity Center と同期されているユーザーとグループがある場合、設定可能な AD Sync の同期スコープには、それらのユーザーとグループのリストがあらかじめ入力されています。新しいユーザーまたはグループを割り当てるには、それらを同期スコープに具体的に追加する必要があります。詳細については、「ユーザーとグループを同期スコープに追加します」を参照してください。

- 新しいユーザーとグループ: 新しいユーザーやグループに AWS アカウント およびアプリケーションへのアクセス権を割り当てる場合は、IAM Identity Center を使用して割り当てを行う前に、設定可能な AD Sync で同期スコープに追加するユーザーとグループを指定する必要があります。詳細については、「ユーザーとグループを同期スコープに追加します」を参照してください。

- Active Directory 内のネストされたグループへの割り当てを行う

  他のグループのメンバーであるグループは、ネストされたグループ (または子グループ) と呼ばれます。ネストされたグループを含む Active Directory のグループに割り当てる場合、割り当てが適用される方法は、AD 同期を使用するか、設定可能な AD 同期を使用するかによって異なります。

  - AD 同期 – ネストされたグループを含む Active Directory 内のグループに割り当てると、グループの直接のメンバーのみがアカウントにアクセスできます。たとえば、グループ A にアクセス権を割り当て、グループ B がグループ A のメンバーである場合、グループ A の直属メンバーのみがアカウントにアクセスできます。グループ B のメンバーはアクセス権を引き継ぎません。
  - 設定可能な AD 同期 — 設定可能な AD 同期を使用して、ネストされたグループを含む Active Directory 内のグループに割り当てると、アプリケーションへのアクセス AWS アカウント またはアプリケーションへのアクセスを持つユーザーのスコープが増大する可能性があります。この場合、割り当ては、ネストされたグループのユーザーを含むすべてのユーザーに適用されます。たとえば、グループ A にアクセス権を割り当て、グループ B がグループ A のメンバーである場合、グループ B のメンバーもこのアクセスを継承します。

- 自動化されたワークフローの更新

  IAM Identity Center ID ストア API アクションと IAM Identity Center 割り当て API アクションを使用して新しいユーザーとグループにアカウントとアプリケーションへのアクセスを割り当て、IAM Identity Center と同期する自動化ワークフローがある場合は、設定可能な AD 同期によって期待どおりに機能するように、2022 年 4 月 15 日までにそれらのワークフローを調整する必要があります。設定可能な AD Sync により、ユーザーとグループの割り当てとプロビジョニングが行われる順序、およびクエリの実行方法が変わります。

  - AD Sync — 割り当てのプロセスが最初に行われます。ユーザーとグループには、アプリケーションへのアクセス AWS アカウント とアプリケーションへのアクセスを割り当てます。ユーザーとグループにアクセス権が割り当てられると、自動的にプロビジョニング (IAM Identity Center に同期) されます。つまり、自動化されたワークフローでは、Active Directory に新しいユーザーを追加すると、自動化されたワークフローが ID ストア `ListUser` API アクションを使用して Active Directory にユーザーを照会し、IAM ID センターの割り当て API アクションを使

用してユーザーアクセスを割り当てることができます。ユーザーには割り当てがあるため、そのユーザーは IAM Identity Center に自動的にプロビジョニングされます。

- 設定可能な AD 同期 — プロビジョニングが最初に実行され、自動的には実行されません。代わりに、まずユーザーとグループを同期スコープに追加して、ID ストアに明示的に追加する必要があります。設定可能な AD Sync の同期設定を自動化するための推奨手順については、同期設定を自動化して、設定可能な AD 同期を実現します。 を参照してください。

設定可能な AD 同期の仕組み

IAM Identity Center は、以下のプロセスで ID ストアの AD ベースの ID データをリフレッシュします。

作成

Active Directory の自己管理型ディレクトリ、または によって管理される AWS Managed Microsoft AD ディレクトリ AWS Directory Service を IAM Identity Center に接続すると、IAM Identity Center ID ストアに同期する Active Directory ユーザーとグループを明示的に設定できます。選択した ID は、3 時間ごとに IAM Identity Center の ID ストアに同期されます。ディレクトリのサイズによっては、同期処理に時間がかかる場合があります。

他のグループのメンバーであるグループ (ネストされたグループまたは子グループ) も ID ストアに書き込まれます。ネストされたグループを含む Active Directory のグループに割り当てる場合、割り当てが適用される方法は、AD 同期を使用するか、設定可能な AD 同期を使用するかによって異なります。詳細については、「Making assignments to nested groups in Active Directory」を参照してください。

新しいユーザーまたはグループが IAM Identity Center アイデンティティストアと同期された後にのみ、アクセス権を割り当てることができます。

更新

IAM Identity Center ID ストアの ID データは、Active Directory のソース ディレクトリから定期的にデータを読み込むことで、常にリフレッシュされた状態を保たれます。IAM Identity Center は、デフォルトで同期サイクルの 1 時間ごとに Active Directory からのデータを同期します。Active Directory のサイズに基づいて、データが IAM Identity Center に同期されるまでに 30 分から 2 時間かかる場合があります。

同期スコープにあるユーザーとグループのオブジェクトとそのメンバーシップは、IAM Identity Center で作成または更新され、Active Directory のソースディレクトリの対応するオブジェクトにマッピングされます。ユーザー属性については、IAM Identity Center コンソールの「アクセス制御用

の属性」セクションにリストされている属性のサブセットのみが IAM Identity Center で更新されます。Active Directory で行った属性更新が IAM Identity Center に反映されるまで、1 つの同期サイクルが必要になる場合があります。

IAM Identity Center ID ストアに同期するユーザーとグループのサブセットを更新することもできます。このサブセットに新しいユーザーまたはグループを追加するか、削除するかを選択できます。追加した ID は、次回の定期同期時に同期されます。サブセットから削除した ID は、IAM Identity Center ID ストアで更新されなくなります。28 日以上同期されていないユーザーは、IAM Identity Center ID ストアで無効になります。対応するユーザーオブジェクトは、同期スコープにまだ含まれている別のグループに属していない限り、次回の同期サイクル時に IAM Identity Center ID ストアで自動的に無効になります。

削除

対応するユーザーまたはグループオブジェクトが Active Directory のソース ディレクトリから削除されると、ユーザーとグループは IAM Identity Center ID ストアから削除されます。または、IAM Identity Center コンソールを使用して IAM Identity Center ID ストアからユーザーオブジェクトを明示的に削除することもできます。IAM Identity Center コンソールを使用する場合は、次回の同期サイクル中に IAM Identity Center に再同期されないように、同期スコープからユーザーを削除する必要もあります。

同期をいつでも一時停止と再開することもできます。28 日以上同期を一時停止すると、すべてのユーザーが無効になります。

同期範囲を設定および管理する

同期スコープは、次のいずれかの方法で設定できます。

- ガイド付きセットアップ: Active Directory から IAM Identity Center にユーザーとグループを初めて同期する場合は、ガイド付きセットアップ の手順に従って同期スコープを設定します。ガイド付きセットアップを完了したら、このセクションの他の手順に従っていつでも同期スコープを変更できます。
- IAM Identity Center と同期されているユーザーとグループがすでにある場合や、ガイド付きセットアップに従いたくない場合は、[同期を管理] を選択します。ガイド付きセットアップ手順をスキップし、必要に応じてこのセクションの他の手順に従って同期スコープを設定および管理してください。

手順

- ガイド付きセットアップ

- ユーザーとグループを同期スコープに追加します
- 同期スコープからユーザーとグループを削除します。
- 同期の一時停止と再開
- 同期の属性マッピングを設定する
- 同期設定を自動化して、設定可能な AD 同期を実現します。

ガイド付きセットアップ

1. IAM Identity Center コンソール を開きます。

> **Note**
>
> 次のステップに進む前に、IAM Identity Center コンソールで AWS Managed Microsoft AD ディレクトリ AWS リージョン がある のいずれかを使用していることを確認してください。

2. [設定] を選択します。
3. ページ上部の通知メッセージで、[ガイド付きセットアップを開始] を選択します。
4. 「ステップ 1 — オプション: 属性マッピングの設定」で、デフォルトのユーザーおよびグループ属性マッピングを確認します。変更が不要な場合は、[次へ] を選択します。変更が必要な場合は、変更を行い、[変更の保存] を選択します。
5. 「ステップ 2 — オプション: 同期範囲の設定」で、「ユーザー」タブを選択します。次に、同期スコープに追加するユーザーの正確なユーザー名を入力し、[追加] を選択します。次に、[グループ] タブを選択します。同期スコープに追加するグループの正確なグループ名を入力し、[追加] を選択します。[次へ] を選択します。後でユーザーとグループを同期スコープに追加する場合は、変更せずに [次へ] を選択します。
6. 「ステップ 3: 設定を確認して保存する」で、「ステップ 1: 属性マッピング」で属性マッピングを確認し、「ステップ 2: 同期スコープ」でユーザーとグループを確認します。[設定の保存] を選択します。これにより、「同期を管理」ページが表示されます。

ユーザーとグループを同期スコープに追加します

ユーザーを追加するには

1. IAM Identity Center コンソール を開きます。

2. [設定] を選択します。
3. 「設定」ページで「ID ソース」タブを選択し、「アクション」を選択し、「同期を管理」を選択します。
4. [同期の管理] ページで、[ユーザー] タブを選択し、[ユーザーとグループの追加] を選択します。
5. [ユーザー] タブの [ユーザー] に正確なユーザー名を入力し、[追加] を選択します。
6. [追加したユーザーとグループ] で、追加するユーザーを確認します。
7. [送信] を選択します。
8. ナビゲーションペインで [Users (ユーザー)] を選択します。
9. 「ユーザー」ページでは、指定したユーザーがリストに表示されるまでに時間がかかる場合があります。ステータスを更新するには、[更新] アイコンをクリックします。

グループを追加するには

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. 「設定」ページで「ID ソース」タブを選択し、「アクション」を選択し、「同期を管理」を選択します。
4. 「同期の管理」ページで「グループ」タブを選択し、「ユーザーとグループの追加」を選択します。
5. [グループ] タブを選択します。[グループ] で、正確なグループ名を入力し、[追加] を選択します。
6. [追加したユーザーとグループ] で、追加するグループを確認します。
7. [送信] を選択します。
8. ナビゲーションペインで、[グループ] を選択します。
9. 「グループ」ページでは、指定したグループがリストに表示されるまでに時間がかかる場合があります。更新アイコンを選択して、グループのリストを更新します。

同期スコープからユーザーとグループを削除します。

同期スコープからユーザーとグループを削除するとどうなるかについての詳細は、設定可能な AD 同期の仕組み を参照してください。

ユーザーを削除するには

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. 「設定」ページで「ID ソース」タブを選択し、「アクション」を選択し、「同期を管理」を選択します。
4. [ユーザー] タブを選択します。
5. [同期範囲のユーザー] で、削除するユーザーの横にあるチェックボックスをオンにします。すべてのユーザーを削除するには、「ユーザー名」の横にあるチェックボックスを選択します。
6. [削除] を選択します。

グループを削除するには

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. 「設定」ページで「ID ソース」タブを選択し、「アクション」を選択し、「同期を管理」を選択します。
4. [グループ] タブを選択します。
5. [同期範囲のグループ] で、削除するユーザーの横にあるチェックボックスをオンにします。すべてのグループを削除するには、[グループ名] の横にあるチェックボックスをオンにします。
6. [削除] を選択します。

同期の一時停止と再開

同期を一時停止すると、今後のすべての同期サイクルが一時停止され、Active Directory 内のユーザーとグループに加えた変更が IAM Identity Center に反映されなくなります。同期を再開すると、同期サイクルでは次に予定されている同期からこれらの変更が反映されます。

同期を一時停止するには

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. 「設定」ページで「ID ソース」タブを選択し、「アクション」を選択し、「同期を管理」を選択します。

4. [同期の管理] で [同期を一時停止] を選択します。

同期を再開するには

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. 「設定」ページで「ID ソース」タブを選択し、「アクション」を選択し、「同期を管理」を選択します。
4. [同期の管理] で [同期を再開] を選択します。

> **Note**
>
> [同期を再開] ではなく [同期を一時停止] が表示される場合は、Active Directory から IAM Identity Center への同期はすでに再開されています。

同期の属性マッピングを設定する

利用可能な属性の詳細については、「AWS Managed Microsoft AD　ディレクトリの属性マッピング」を参照してください。

IAM Identity Center でディレクトリへの属性マッピングを設定するには

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. 「設定」ページで「ID ソース」タブを選択し、「アクション」を選択し、「同期を管理」を選択します。
4. 「同期の管理」で、「属性マッピングを表示」を選択します。
5. 「Active Directory ユーザー属性」で、IAM Identity Center ID ストア属性 とActive Directory のユーザー属性を設定します。例えば、IAM Identity Center ID ストア属性 `email` を Active Directory のユーザーディレクトリ属性 `${objectguid}` にマップすることができます。

> **Note**
>
> 「グループ属性」では、IAM Identity Center の ID ストア属性 とActive Directory グループの属性 は変更できません。

6. [変更の保存] を選択します。これにより、「同期の管理」ページに戻ります。

同期設定を自動化して、設定可能な AD 同期を実現します。

設定可能な AD 同期で自動化されたワークフローが期待どおりに機能するようにするには、次の手順を実行して同期設定を自動化することをお勧めします。

設定可能な AD Sync の同期設定を自動化するには

1. Active Directory で、IAM Identity Center に同期したいすべてのユーザーとグループを含む 親同期グループを作成します。例えば、グループ IAMIdentityCenterAllUsersAndGroups に名前を付けることができます。
2. IAM Identity Center で、親同期グループを設定可能な同期リストに追加します。IAM Identity Center は、親同期グループに含まれるすべてのユーザー、グループ、サブグループ、およびすべてのグループのメンバーを同期します。
3. Microsoft が提供する Active Directory ユーザーおよびグループ管理 API アクションを使用して、親同期グループにユーザーとグループを追加または削除します。

IAM Identity Center AD 同期

IAM Identity Center AD 同期では、IAM Identity Center を使用して、Active Directory のユーザーとグループに、 AWS マネージドアプリケーションまたはカスタマーマネージドアプリケーションへのアクセス AWS アカウント 許可を割り当てます。割り当てられた ID はすべて IAM Identity Center に自動的に同期されます。

IAM Identity Center AD 同期の仕組み

IAM Identity Center は、以下のプロセスで ID ストアの AD ベースの ID データを更新します。

作成

コンソールまたは割り当て API コールを使用して AWS ユーザー AWS アカウント またはグループを またはアプリケーションに割り当てると、ユーザー、グループ、メンバーシップに関する情報が IAM Identity Center アイデンティティストアに定期的に同期されます。IAM Identity Center の割り当てに追加されたユーザーまたはグループは、通常 2 時間以内に AWS ID ストアに表示されます。同期されるデータの量によっては、この処理に時間がかかる場合があります。同期されるのは、アクセス権が直接割り当てられているか、アクセス権が割り当てられているグループのメンバーであるユーザーとグループのみです。

他のグループメンバーであるグループ (ネストされたグループと呼ばれる) も、ID ストアに書き込まれます。ネストされたグループを含む Active Directory のグループに割り当てる場合、割り当てが適用される方法は、AD 同期を使用するか、設定可能な AD 同期を使用するかによって異なります。

- AD 同期 – ネストされたグループを含む Active Directory 内のグループに割り当てると、グループの直接のメンバーのみがアカウントにアクセスできます。たとえば、グループ A にアクセス権を割り当て、グループ B がグループ A のメンバーである場合、グループ A の直属メンバーのみがアカウントにアクセスできます。グループ B のメンバーはアクセス権を引き継ぎません。
- 設定可能な AD 同期 — 設定可能な AD 同期を使用して、ネストされたグループを含む Active Directory 内のグループに割り当てると、アプリケーションへのアクセス AWS アカウント またはアプリケーションへのアクセスを持つユーザーのスコープが増大する可能性があります。この場合、割り当ては、ネストされたグループのユーザーを含むすべてのユーザーに適用されます。たとえば、グループ A にアクセス権を割り当て、グループ B がグループ A のメンバーである場合、グループ B のメンバーもこのアクセスを継承します。

ユーザーオブジェクトが初めて同期される前にユーザーが IAM Identity Center にアクセスする場合、そのユーザーの ID ストアオブジェクトは (JIT) プロビジョニングを使用して just-in-timeオンデマンドで作成されます。JIT プロビジョニングによって作成されたユーザーは、直接割り当てられた、またはグループベースの IAM Identity Center エンタイトルメントがない限り、同期されません。JIT でプロビジョニングされたユーザーのグループメンバーシップは、同期化されるまで利用できません。

ユーザーに へのアクセスを割り当てる方法については AWS アカウント、「」を参照してくださいへのシングルサインオンアクセス AWS アカウント。

更新

IAM Identity Center ID ストアの ID データは、Active Directory のソース ディレクトリから定期的にデータを読み込むことで、常にリフレッシュされた状態を保たれます。Active Directory で変更された ID データは、通常 4 時間以内に AWS ID ストアに表示されます。同期されるデータの量によっては、この処理に時間がかかる場合があります。

ユーザーとグループのオブジェクトとそのメンバーシップは、IAM Identity Center で作成または更新され、Active Directory のソースディレクトリで対応するオブジェクトにマッピングされます。ユーザー属性については、IAM Identity Center コンソールの「アクセスコントロール用の属性の管理」セクションにリストされている属性のサブセットのみが IAM Identity Center で更新されます。さらに、ユーザー属性は、各ユーザー認証イベントで更新されます。

削除

対応するユーザーまたはグループオブジェクトが Active Directory のソース ディレクトリから削除されると、ユーザーとグループは IAM Identity Center ID ストアから削除されます。

外部 ID プロバイダに接続する方法には

Active Directory または でセルフマネージドディレクトリを使用している場合は AWS Managed Microsoft AD、「」を参照してくださいMicrosoft AD ディレクトリへの接続。他の外部 ID プロバイダー (IdPs) の場合 AWS IAM Identity Center 、 を使用して、Security Assertion Markup Language (SAML) 2.0 標準 IdPs を通じて から ID を認証できます。これにより、ユーザーは会社の認証情報を使用して AWS アクセスポータルにサインインできます。その後、外部 でホストされている割り当てられたアカウント、ロール、アプリケーションに移動できます IdPs。

例えば、Okta や Microsoft Entra ID などの外部 IdP を IAM アイデンティティセンターに接続できます。その後、ユーザーは既存の Oktaまたは Microsoft Entra ID認証情報を使用して AWS アクセスポータルにサインインできます。ユーザーがサインインした後に実行できる操作を制御するには、 AWS 組織内のすべてのアカウントとアプリケーションにわたってアクセス許可を一元的に割り当てることができます。さらに、デベロッパーは既存の認証情報を使用して AWS Command Line Interface （ AWS CLI) にサインインするだけで、短期的な認証情報の自動生成とローテーションのメリットを得ることができます。

SAML プロトコルは、ユーザーやグループについての情報を得るために IdP へクエリする方法は提供していません。そのため、IAM Identity Center がこれらのユーザーやグループを IAM Identity Center にプロビジョニングして認識する必要があります。

ユーザーが外部の IdP から来た場合のプロビジョニング

外部 IdP を使用する場合は、 AWS アカウント またはアプリケーションに割り当てる前に、該当するすべてのユーザーとグループを IAM Identity Center にプロビジョニングする必要があります。これを行うには、ユーザーやグループに合わせて 自動プロビジョニング を設定するか、手動のプロビジョニング を使用します。ユーザーのプロビジョニング方法に関係なく、IAM Identity Center は、AWS Management Console、コマンドラインインターフェイス、およびアプリケーション認証を外部 IdP にリダイレクトします。IAM Identity Center では、IAM Identity Center センターで作成したポリシーに基づいて、それらのリソースへのアクセス権を付与します。プロビジョニングの詳細については、「ユーザーおよびグループのプロビジョニング」を参照してください。

外部 ID プロバイダに接続する方法

サポートされている の step-by-step チュートリアルがあります IdPs。

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

サポートされている外部 には、さまざまな前提条件、考慮事項、プロビジョニング手順がありますIdPs。以下の手順は、すべての外部 ID プロバイダーで使用される手順の概要を示しています。

外部 ID プロバイダに接続する方法には

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. [設定] ページで [ID ソース] タブを選択し、[アクション] > [ID ソースを変更]を選択します。
4. [ID ソースの選択] で [外部 ID プロバイダー] を選択し、[次へ] を選択します。
5. [外部 ID プロバイダーの設定] で、次の操作を行います。

    a. [サービスプロバイダーメタデータ] で、[Download metadata file] (メタデータファイルのダウンロード) を選択すると、メタデータファイルがダウンロードされ、システムに保存されます。IAM Identity Center SAML メタデータファイルは、外部の ID プロバイダーに必要です。

    b. [ID プロバイダのメタデータ] で、[ファイルを参照] を選択し、外部の ID プロバイダからダウンロードしたメタデータファイルを検索します。次に、ファイルをアップロードします。このメタデータファイルには，IdP から送信されるメッセージを信頼を得るための公開 x509 証明書が含まれています。

    c. [次へ] をクリックします。

> **Important**
>
> ソースをアクティブディレクトリとの間で変更すると、既存のユーザーやグループの割り当てがすべて削除されます。ソースの変更が成功したら、手動で割り当てを再適用する必要があります。

6. 免責事項を読み、次に進む準備ができたら、[ACCEPT] (許諾) を押してください。
7. [Change identity source] (ID ソースの変更) を選択します。ID ソースを正常に変更したことを知らせるメッセージが表示されます。

トピック

- 外部 ID プロバイダーでの SAML および SCIM ID フェデレーションの使用
- SCIM プロファイルおよび SAML 2.0 の実装

外部 ID プロバイダーでの SAML および SCIM ID フェデレーションの使用

IAM Identity Center は、ID フェデレーションのために以下の標準ベースのプロトコルを実装しています。

- ユーザー認証用の SAML 2.0
- SCIM のプロビジョニング

これらの標準的なプロトコルを実装している ID プロバイダー (IdP) は、以下の特別な注意事項を除き、IAM Identity Center と正常に相互運用できると考えられます。

- SAML
  - IAM Identity Center では、SAML の nameID 形式のメールアドレス (つまり `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`) が必要です。
  - アサーションの nameID フィールドの値は、RFC 2822 (https://tools.ietf.org/html/rfc2822) addr-spec 準拠 (“`name@domain.com`”) 文字列 (https://tools.ietf.org/html/rfc2822#section-3.4.1) である必要があります。
  - メタデータファイルは 75000 文字を超えることはできません。
  - メタデータには、サインイン URL の一部として entityId 、X509 証明書、 SingleSignOnService が含まれている必要があります。
  - 暗号化キーはサポートされていません。

- SCIM
  - IAM Identity Center SCIM の実装は、SCIM RFCs 7642 (https://tools.ietf.org/html/rfc7642)、7643 (https://tools.ietf.org/html/rfc7643)、および 7644 (https://tools.ietf.org/html/rfc7644) と、2020 年 3 月の FastFed 基本的な SCIM プロファイル 1.0 (https://openid.net/specs/

fastfed-scim-1_0-02.html#rfc.section.4) のドラフトで説明されている相互運用性要件に基づいています。これらのドキュメントと現在の IAM Identity Center での実装との違いは、「IAM Identity Center SCIM 実装デベロッパーガイドの「サポートされる API オペレーション」のセクションに記載されています。

IdPs 上記の標準および考慮事項に準拠していない はサポートされていません。これらの規格や注意事項への製品の適合性に関する質問や説明については、お客様の IdP にお問い合わせください。

お使いの IdP と IAM Identity Center の接続に問題がある場合は、以下を確認することをお勧めします。

- AWS CloudTrail イベント名 ExternalIdPDirectoryLogin でフィルタリングして ログを記録する
- IdP 固有のログやデバッグログ
- IAM Identity Center の問題のトラブルシューティング

> **Note**
>
> の など IdPs、一部の では入門チュートリアル、IAM Identity Center 用に特別に構築された「アプリケーション」または「コネクタ」の形式で IAM Identity Center の設定を簡素化できます。お使いの IdP がこのオプションを提供している場合は、IAM Identity Center 用に作成されたアイテムを慎重に選択して使用することをお勧めします。AWS「」、AWS 「フェデレーション」、または類似の一般的なAWS「」名と呼ばれる他の項目は、他のフェデレーションアプローチやエンドポイントを使用する可能性があり、IAM Identity Center では期待どおりに動作しない場合があります。

SCIM プロファイルおよび SAML 2.0 の実装

SCIM および SAML は共に IAM Identity Center を構成する上で重要な注意事項です。

SAML 2.0 の実装

IAM Identity Center は、SAML (Security Assertion Markup Language) 2.0 との ID フェデレーションをサポートします。これにより、IAM Identity Center は外部 ID プロバイダー () からの ID を認証できますIdPs。SAML 2.0 は、SAML アサーションを安全に交換するためのオープンスタンダードです。SAML 2.0 は、SAML 権限 (ID プロバイダ (IdP) と呼ばれます) と SAML コンシューマ (サービスプロバイダ (SP) と呼ばれます) の間で、ユーザに関する情報を渡します。IAM Identity Center サービ

スは、この情報を使って、フェデレーテッドシングルサインオン (SSO) を提供します。シングルサインオンを使用すると、ユーザーは既存の ID プロバイダーの認証情報に基づいて AWS アカウントおよび設定されたアプリケーションにアクセスできます。

IAM Identity Center は、IAM Identity Center ストア AWS Managed Microsoft ADまたは外部 ID プロバイダーに SAML IdP 機能を追加します。その後、ユーザーは、、、 などの AWS Management Console およびサードパーティーアプリケーションを含む SAML をサポートするサービスにシングルサインオンできますMicrosoft 365ConcurSalesforce。

しかし、SAML プロトコルは、ユーザーやグループについての情報を得るために IdP へクエリする方法は提供していません。そのため、IAM Identity Center がこれらのユーザーやグループを IAM Identity Center にプロビジョニングして認識する必要があります。

SCIM プロファイル

IAM Identity Center は、クロスドメインアイデンティティ管理システム (SCIM) v2.0 規格に対応しています。SCIM は、IAM Identity Center の ID と IdP の ID を同期させます。これには、IdP と IAM Identity Center の間で行われるユーザーのプロビジョニング、アップデート、デプロビジョニングが含まれます。

SCIM を実装する方法の詳細については、「自動プロビジョニング」を参照してください。IAM Identity Center の SCIM 実装の詳細については、「IAM Identity Center SCIM 実装デベロッパーガイド」() を参照してください。

トピック

- 自動プロビジョニング
- 手動のプロビジョニング
- SAML 2.0 証明書の管理

自動プロビジョニング

IAM Identity Center は、クロスドメインアイデンティティ管理システム (SCIM) v2.0 プロトコルを使用して、ID プロバイダー (IdP) から IAM Identity Center へのユーザーおよびグループ情報の自動プロビジョニング (同期化) をサポートしています。SCIM 同期を設定すると、ID プロバイダー (IdP) のユーザー属性と IAM Identity Center の名前付き属性のマッピングが作成されます。これにより、IAM Identity Center とお客様の IdP の間で、期待される属性が一致します。この接続を IdP で設定するには、IAM Identity Center 用の SCIM エンドポイントと IAM Identity Center で作成したベアラートークンを使用します。

トピック

- 自動プロビジョニングを使用する際の注意事項
- アクセストークンの有効期限を監視する方法
- 自動プロビジョニングを有効にする方法
- 自動プロビジョニングを無効にする方法
- 新しいアクセストークンを生成する方法
- アクセストークンを削除する方法
- アクセストークンをローテーションする方法

自動プロビジョニングを使用する際の注意事項

SCIM のデプロイを開始する前に、まず、IAM Identity Center との連携について、以下の注意事項を確認することをお勧めします。プロビジョニングに関するその他の考慮事項については、IdP 入門チュートリアルに適用される を参照してください。

- プライマリの E メールアドレスをプロビジョニングする場合、この属性値は各ユーザーに対して一意でなければなりません。一部の では IdPs、プライマリ E メールアドレスが実際の E メールアドレスではない場合があります。例えば、E メールにしか見えない UPN (Universal Principal Name) だったりします。これらには、ユーザーの実際の E メールアドレスを含むセカンダリまたは「その他」の E メールアドレスが含まれる IdPs 場合があります。Null 以外の一意なメールアドレスを IAM Identity Center のプライマリ E メールアドレス属性にマッピングするために、IdP の SCIM を設定する必要があります。また、ユーザーの Null 以外の一意なサインイン識別子を IAM Identity Center のユーザー名属性にマッピングする必要があります。ご利用の IdP に、サインイン識別子とユーザーの E メール名を兼ねた単一の値があるかどうかを確認してください。その場合、その IdP フィールドを IAM Identity Center のプライマリ E メールと IAM Identity Center のユーザー名の両方にマッピングすることができます。
- SCIM の同期が機能するためには、すべてのユーザーが First name (名)、Last name (姓)、Username (ユーザーネーム)、Display name (表示名) の値を指定する必要があります。これらのすべての値が設定されていないユーザーはプロビジョニングされません。
- サードパーティーのアプリケーションを使用する必要がある場合は、まず、アウトバウンド SAML のサブジェクト属性をユーザー名属性にマッピングする必要があります。サードパーティーのアプリケーションにルーティング可能な E メールアドレスが必要な場合、E メール属性を IdP に提供する必要があります。
- SCIM のプロビジョニングとアップデートの間隔は、ID プロバイダーによって管理されます。ID プロバイダーのユーザーおよびグループに対する変更は、ID プロバイダーがそれらの変更を IAM

Identity Center に送信した後に、 SSO にのみ反映されます。ユーザーやグループの更新の頻度については、ID プロバイダーにご確認ください。

- 現在、SCIM では多値属性 (特定のユーザーに対する複数の E メールや電話番号など) は提供されていません。SCIM を使用した IAM Identity Center に多値属性を同期させようとすると失敗します。失敗を回避するために、各属性には 1 つの値しか渡さないようにします。マルチバリューの属性を持つユーザーがいる場合は、IAM Identity Center への接続のために、IdP の SCIM で重複する属性マッピングを削除または変更します。
- お客様の IdP での `externalId` SCIM マッピングが、一意で常に存在し、お客様のユーザにとって変更の可能性が低い値に対応していることを確認してください。例えば、IdP は、名前や E メールなどのユーザー属性の変更に影響されない、保証付きの `objectId` やその他の識別子を提供することができます。そうであれば、その値を SCIM の `externalId` フィールドにマッピングすることができます。これにより、名前や E メールを変更する必要がある場合に、ユーザーが AWS 使用権限、割り当て、アクセス許可を失うことがなくなります。
- まだアプリケーションに割り当てられていないユーザー、または IAM Identity Center にプロビジョニング AWS アカウント できないユーザー。ユーザーとグループを同期させるには、ユーザーとグループが、IAM Identity Center への IdP の接続を表すアプリケーションやその他の設定に割り当てられていることを確認してください。
- ユーザーのプロビジョニング解除の動作は ID プロバイダーによって管理され、実装によって異なる場合があります。ユーザーのプロビジョニング解除の詳細については、ID プロバイダーにお問い合わせください。

IAM Identity Center の SCIM 実装の詳細については、「IAM Identity Center SCIM 実装デベロッパーガイド」() を参照してください。

アクセストークンの有効期限を監視する方法

SCIM アクセストークンは 1 年の有効期間で生成されます。SCIM アクセストークンが 90 日以内に期限切れに設定されている場合、 はトークンのローテーションに役立つ AWS リマインダーを IAM Identity Center コンソールと AWS Health Dashboard に送信します。SCIM アクセストークンを有効期限が切れる前にローテーションすることで、ユーザーとグループの情報の自動プロビジョニングを継続的に保護できます。SCIM アクセストークンの有効期限が切れると、ID プロバイダーから IAM Identity Center へのユーザーとグループの情報の同期が停止するため、自動プロビジョニングでは情報を更新したり、情報を作成、削除したりできなくなります。自動プロビジョニングが中断されると、セキュリティリスクが高まり、サービスへのアクセスに影響が及ぶ可能性があります。

Identity Center コンソールのリマインダーは、SCIM アクセストークンをローテーションして、未使用または期限切れのアクセストークンを削除するまで続きます。 AWS Health ダッシュボードイベン

トは、SCIM アクセストークンの有効期限が切れるまで、90 日から 60 日の間は毎週 2 回、60 日から 30 日の間は毎週 3 回、30 日から 15 日の間は毎日更新されます。

自動プロビジョニングを有効にする方法

SCIM プロトコルを使用して、IdP から IAM Identity Center へのユーザーおよびグループの自動プロビジョニングを有効にするには、以下の手順を使用します。

> **Note**
>
> この手順を開始する前に、まずお客様の IdP に適用されるプロビジョニングに関する注意事項を確認することをお勧めします。詳細については、IdP の入門チュートリアル「」を参照してください。

IAM Identity Center で自動プロビジョニングを有効にするには

1. 前提条件が整ったら、IAM Identity Center コンソールを開きます。
2. 左側のナビゲーションペインの [Settings] (設定) を選択します。
3. [設定] ページで、[自動プロビジョニング] 情報ボックスを探し、[有効化] を選択します。これにより、すぐに IAM Identity Center の自動プロビジョニングが有効になり、必要なエンドポイントとアクセストークンの情報が表示されます。
4. [Inbound automatic provisioning] (インバウンド自動プロビジョニング) ダイアログボックスで、以下のオプションの値をそれぞれコピーします。これらは、後で IdP でプロビジョニングを設定する際に貼り付ける必要があります。
   a. SCIM エンドポイント
   b. アクセストークン
5. [Close] (閉じる) を選択します。

この手順が完了したら、IdP で自動プロビジョニングを設定する必要があります。詳細については、IdP の入門チュートリアル「」を参照してください。

自動プロビジョニングを無効にする方法

以下の手順で、IAM Identity Center コンソールでの自動プロビジョニングを無効にします。

> **Important**
>
> この手順を行う前にアクセストークンを削除する必要があります。詳細については、「アクセストークンを削除する方法」を参照してください。

IAM Identity Center コンソールで自動プロビジョニングを無効にするには

1. [IAM Identity Center コンソール] で、左のナビゲーションペインの [設定] を選択します。
2. [設定] ページで [ID ソース] タブを選択し、[アクション] > [プロビジョニングの管理] を選択します。
3. [自動プロビジョニング] ページで、[無効にする] を選択します。
4. [Disable automatic provisioning] (自動プロビジョニングを無効にする) ダイアログボックスで、情報を確認し、[DISABLE] (無効) と入力して、[Disable automatic provisioning] (自動プロビジョニングを無効にする) を選択します。

新しいアクセストークンを生成する方法

以下の手順で、IAM Identity Center コンソールで新しいアクセストークンを生成します。

> **Note**
>
> この手順では、自動プロビジョニングが事前に有効になっている必要があります。詳細については、「自動プロビジョニングを有効にする方法」を参照してください。

新しいアクセストークンを生成するには

1. [IAM Identity Center コンソール] で、左のナビゲーションペインの [設定] を選択します。
2. [設定] ページで [ID ソース] タブを選択し、[アクション] > [プロビジョニングの管理] を選択します。
3. [自動プロビジョニング] ページで、 [アクセストークン] の [トークンを生成する] を選択します。
4. [新しいアクセストークンを生成] ダイアログで、新しいアクセストークンをコピーして安全な場所に保存します。
5. [閉じる] を選びます。

アクセストークンを削除する方法

以下の手順で、IAM Identity Center コンソールで既存のアクセストークンを削除します。

既存のアクセストークンを削除するには

1. [IAM Identity Center コンソール] で、左のナビゲーションペインの [設定] を選択します。
2. [設定] ページで [ID ソース] タブを選択し、[アクション] > [プロビジョニングの管理] を選択します。
3. [自動プロビジョニング] ページで、[アクセストークン] から削除したいアクセストークンを選び、[削除] を選択します。
4. [Delete access token] (アクセストークンを削除する) ダイアログボックスで、情報を確認し、[DELETE] (削除) と入力して、[Delete access token] (アクセストークンを削除する) を選択します。

アクセストークンをローテーションする方法

IAM Identity Center ディレクトリは一度に 2 つまでのアクセストークンをサポートします。ローテーションの前に追加のアクセストークンを生成するには、期限切れまたは未使用のアクセストークンをすべて削除します。

SCIM アクセストークンの有効期限が近づいている場合は、以下の手順で IAM Identity Center コンソールで既存のアクセストークンをローテーションさせることができます。

アクセストークンをローテーションするには

1. [IAM Identity Center コンソール] で、左のナビゲーションペインの [設定] を選択します。
2. [設定] ページで [ID ソース] タブを選択し、[アクション] > [プロビジョニングの管理] を選択します。
3. [Automatic provisioning] (自動プロビジョニング) ページの [Access Token] (アクセストークン) でローテーションさせたいトークンのトークン ID をメモしておきます。
4. 新しいアクセストークンを生成する方法 の手順に従って、新しいトークンを作成します。既に最大数の SCIM アクセストークンを作成している場合は、まず既存のトークンの 1 つを削除する必要があります。
5. ID プロバイダーのウェブサイトにアクセスし、新しいアクセストークンを SCIM プロビジョニング用に設定した後、新しい SCIM アクセストークンを使用して IAM Identity Center への接続

をテストします。新しいトークンを使ってプロビジョニングが正常に行われていることを確認したら、この手順の次のステップに進みます。

6. アクセストークンを削除する方法 の手順で、先ほどの古いアクセストークンを削除します。また、どのトークンを削除するかを判断するために、トークンの作成日を利用することもできます。

手動のプロビジョニング

一部の では、クロスドメインアイデンティティ管理 (SCIM) がサポートされ IdPs ていないか、互換性のない SCIM 実装があります。そのような場合は、IAM Identity Center コンソールを通じて手動でユーザーをプロビジョニングすることができます。IAM Identity Center にユーザーを追加する際には、IdP に登録されているユーザー名と同一のユーザー名を設定します。少なくとも、一意の E メールアドレスとユーザー名が必要です。詳細については、「ユーザー名と E メールアドレスの一意性」を参照してください。

また、IAM Identity Center では、すべてのグループを手動で管理する必要があります。そのためには、グループを作成し、IAM Identity Center コンソールを使ってグループを追加します。これらのグループは、お客様の IdP に存在するものと一致する必要はありません。詳細については、「グループ」を参照してください。

SAML 2.0 証明書の管理

IAM ID Center は、証明書を使用して、外部 ID プロバイダー (IdP)と IAM Identity Center との間の SAML 信頼関係を確立します。IAM Identity Center で外部 IdP を追加する際には、外部 IdP から少なくとも 1 つの SAML 2.0 X.509 のパブリック証明書を取得する必要があります。その証明書は、通常、信頼を作成中の IdP SAML メタデータ交換時に自動的にインストールされます。

IAM Identity Center の管理者として、古い IdP 証明書を新しい証明書に置き換える必要がある場合があります。例えば、IdP 証明書の有効期限が近づいている場合は、証明書を交換する必要があります。古い証明書を新しい証明書に置き換えるプロセスは、証明書のローテーションと呼ばれています。

トピック

- SAML 2.0 証明書をローテーションする
- 証明書の有効期限切れステータスインジケーター

SAML 2.0 証明書をローテーションする

ID プロバイダーが発行した無効または期限切れの証明書をローテーションさせるために、定期的に証明書をインポートする必要がある場合があります。これにより、認証の乱れやダウンタイムを防ぐことができます。インポートされた証明書はすべて自動的に有効になります。証明書の削除は、関連する ID プロバイダで使用されなくなったことを確認した後に行います。

また、一部の は複数の証明書をサポートしていない IdPs 可能性があることも考慮する必要があります。この場合、これらを使用して証明書をローテーションする行為は、ユーザーにとって一時的なサービスの中断を意味する IdPs 可能性があります。その IdP との信頼関係が正常に再構築されたときに、サービスが再開されます。このオペレーションは、ピーク時を可能な限り避けて慎重に計画してください。

> **Note**
>
> セキュリティのベストプラクティスとして、既存の SAML 証明書に不正アクセスや不適切な取り扱いがあった場合には、直ちに証明書を削除してローテーションする必要があります。

IAM Identity Center 証明書のローテーションは、以下の複数のステップで行われます。

- IdP から新しい証明書を取得する
- 新しい証明書を IAM Identity Center にインポートする
- IdP での新しい証明書を有効にする
- 古い証明書を削除する

以下のすべての手順を使用して、認証のダウンタイムを回避しながら、証明書のローテーションプロセスを完了します。

ステップ 1: IdP から新しい証明書を取得する

IdP の ウェブサイトにアクセスして、SAML 2.0 証明書をダウンロードします。証明書ファイルが PEM エンコード形式でダウンロードされていることを確認してください。ほとんどのプロバイダでは、IdP に複数の SAML 2.0 証明書を作成することができます。これらは、無効や非アクティブとしてマークされている可能性があります。

ステップ 2: IAM Identity Center にインポートする

以下の手順で、IAM Identity Center コンソールを使って新しい証明書をインポートします。

1. [IAM Identity Center コンソール] で [設定] を選択します。
2. [設定] ページで [ID ソース] タブを選択し、[アクション] > [認証の管理] を選択します。
3. [SAML 2.0 認証の管理] ページで、[証明書のインポート] を選択します。
4. [SAML 2.0 証明書のインポート] ダイアログで、[ファイルを選択] を選択し、証明書ファイルに移動して選択し、[証明書のインポート] を選択します。

この時点で、IAM Identity Center は、お客様がインポートした両方の証明書から署名されたすべての受信 SAML メッセージを信頼します。

ステップ 3: IdP で新しい証明書を有効にする

IdP の ウェブサイトに戻り、先ほど作成した新しい証明書をプライマリまたはアクティブとしてマークします。この時点で、IdP が署名したすべての SAML メッセージは、新しい証明書を使用する必要があります。

ステップ 4: 古い証明書を削除する

以下の手順で、IdP の証明書ローテーション処理を行います。少なくとも 1 つの有効な証明書が必要であり、それを削除することはできません。

> **Note**
>
> この証明書を削除する前に、ID プロバイダがこの証明書を使用して SAML レスポンスに署名しなくなったことを確認します。

1. リポジトリの [Manage SAML 2.0 certificates] (SAML 2.0 証明書の管理) ページで、削除する証明書を選択します。[Delete] (削除) を選択します。
2. [Delete SAML 2.0 certificate] (SAML 2.0 証明書の削除) ダイアログボックスで、**DELETE** をタイプして確認し、[Delete] (削除) を選択します。
3. IdP のウェブサイトに戻り、古い非アクティブな証明書を削除するために必要な手順を実行します。

証明書の有効期限切れステータスインジケーター

[Manage SAML 2.0 certificates] (SAML 2.0証明書の管理) ページでは、色付きのステータスインジケータアイコンが表示されることがあります。これらのアイコンは、リストの各証明書の横にある

[Expires on] (有効期限) 列に表示されます。以下は、IAM Identity Center が各証明書に対してどのアイコンを表示するかを決定するための基準です。

- 赤 — 証明書が現在期限切れであることを示します。
- 黄 — 証明書の有効期限が 90 日以下であることを示します。
- 緑 — 証明書が現在有効であり、少なくとも 90 日間有効であることを示します。

証明書の現在のステータスを確認するには

1. [IAM Identity Center コンソール] で [設定] を選択します。
2. [設定] ページで [ID ソース] タブを選択し、[アクション] > [認証の管理] を選択します。
3. [SAML 2.0 証明書の管理] ページの [SAML 2.0 証明書の管理] で、リストの証明書のステータスを [有効期限] 欄に表示します。

AWS アクセスポータルの使用

AWS アクセスポータルでは、Office 365、Concur、Salesforce など、すべての AWS アカウント および最も一般的に使用されるクラウドアプリケーションへのシングルサインオンアクセスをユーザー (エンドユーザー) に提供します。ポータル内から、 AWS アカウント またはアプリケーションのアイコンを選択するだけで、複数のアプリケーションをすばやく起動できます。 AWS アクセスポータルにアプリケーションアイコンが存在するということは、会社の管理者がそれらの AWS アカウント またはアプリケーションへのアクセスを許可していることを意味します。また、追加のサインインプロンプトなしで、 AWS アクセスポータルからこれらのアカウントまたはアプリケーションすべてにアクセスできることも意味します。

以下の状況では、管理者に連絡して追加のアクセスをリクエストしてください。

- アクセスする必要がある AWS アカウント またはアプリケーションが表示されません。
- 特定のアカウントまたはアプリケーションに対するアクセス権が期待どおりではありません。

トピック

- IAM Identity Center への参加招待を受け入れる
- AWS アクセスポータルにサインインする
- IAM Identity Center でユーザーのパスワードをリセットする手順
- AWS CLI または AWS SDKs

- AWS Management Console 送信先へのショートカットリンクの作成
- MFA 用デバイスの登録
- AWS アクセスポータル URL のカスタマイズ

IAM Identity Center への参加招待を受け入れる

AWS アクセスポータルに初めてサインインする場合は、E メールをチェックしてユーザー認証情報をアクティブ化する手順を確認してください。

ユーザー認証情報を有効にするには

1. 会社から受け取った E メールに応じて、次のいずれかの方法を選択してユーザー認証情報をアクティブ化し、 AWS アクセスポータルの使用を開始できるようにします。

   a. AWS 「IAM Identity Center への参加の招待」 (AWS シングルサインオンの後継) という件名の E メールを受信した場合は、そのメールを開き、招待を受け入れる」を選択します。「新規ユーザー登録」ページで、パスワードを入力して確認し、「新しいパスワードを設定」を選択します。このパスワードは、ポータルにサインインするたびに使用します。

   b. 貴社の IT サポートまたは IT 管理者から E メールを送信された場合は、ユーザー認証情報をアクティブ化するために伝えられた指示事項に従います。

2. 新しいパスワードを指定してユーザー認証情報をアクティブ化すると、 AWS アクセスポータルは自動的にサインインします。されない場合は、次のステップで説明されている指示事項に従って、手動で AWS アクセスポータルにサインインできます。

AWS アクセスポータルにサインインする

この時点で、管理者から AWS アクセスポータルへの特定のサインイン URL が提供されているはずです。この URL があれば、以下の手順を実行してポータルにサインインできます。詳細については、AWS 「 アクセスポータルにサインインする」を参照してください。

> **Note**
>
> サインイン後、 AWS アクセスポータルセッションのデフォルトの期間は 8 時間です。管理者はこのセッションの期間を変更できることに注意してください。

信頼されたデバイス

サインインページで [これは信頼できるデバイスです] というオプションを選択すると、IAM Identity Center はそのデバイスからの今後のすべてのサインインを承認されたものとみなします。つまり、その信頼できるデバイスを使用している限り、IAM Identity Center は、MFA コードを入力する指示を出しません。ただし、新しいブラウザからサインインした場合や、お客様のデバイスに未知の IP アドレスが発行された場合などは例外となります。

AWS アクセスポータルへのサインインのヒント

AWS アクセスポータルエクスペリエンスの管理に役立つヒントをいくつか紹介します。

- 場合によっては、サインアウトして AWS アクセスポータルに再度サインインする必要があります。この手順は、管理者から最近割り当てられた新しいアプリケーションにアクセスするために必要になります。ただし、すべての新しいアプリケーションは 1 時間ごとに更新されるため、この手順は必須ではありません。
- AWS アクセスポータルにサインインすると、アプリケーションのアイコンを選択して、ポータルにリストされている任意のアプリケーションを開くことができます。アプリケーションの使用が完了したら、アプリケーションを閉じるか、 AWS アクセスポータルからサインアウトできます。アプリケーションを閉じると、そのアプリケーションからのみサインアウトされます。 AWS アクセスポータルから開いた他のアプリケーションは、開いたままで実行されています。
- 別のユーザーとしてサインインするには、最初に AWS アクセスポータルからサインアウトする必要があります。ポータルからログアウトすると、ブラウザセッションから認証情報が完全に削除されます。
- AWS アクセスポータルにサインインしたら、ロールに切り替えることができます。切り替えることで元のユーザーアクセス権限が一時的に無効になり、そのロールに割り当てられたアクセス権限が代わりに付与されます。 詳細については、「ロールの切り替え (コンソール)」を参照してください。

AWS アクセスポータルからのサインアウト

ポータルからログアウトすると、認証情報がブラウザセッションから完全に削除されます。詳細については、 AWS サインインガイドの AWS 「 アクセスポータルからサインアウトする」を参照してください。

AWS アクセスポータルからサインアウトするには

- AWS アクセスポータルで、ナビゲーションバーからサインアウトを選択します。

> **Note**
>
> 別のユーザーとしてサインインする場合は、最初に AWS アクセスポータルからサインアウトする必要があります。

IAM Identity Center でユーザーのパスワードをリセットする手順

AWS アクセスポータルでは、IAM Identity Center ユーザーは、ウェブポータルを通じて、割り当てられたすべての AWS アカウントとクラウドアプリケーションへのシングルサインオンアクセスが可能になります。 AWS アクセスポータルはAWS Management Console、 AWS リソースを管理するためのサービスコンソールのコレクションである とは異なります。

この手順を使用して、 AWS アクセスポータルの IAM Identity Center ユーザーパスワードをリセットします。ユーザータイプの詳細については、「AWS サインイン ユーザーガイド」をご覧ください。

考慮事項

AWS アクセスポータルのパスワードリセット機能は、Identity Center ディレクトリを使用している、または ID ソースAWS Managed Microsoft ADとして Identity Center インスタンスのユーザーのみが使用できます。ユーザーが外部 ID プロバイダーまたは AD Connector に接続されている場合、ユーザーパスワードのリセットは外部 ID プロバイダーまたは接続された から行う必要がありますActive Directory。

- ID ソースが IAM Identity Center ディレクトリの場合は、「」を参照してくださいIAM Identity Center で ID を管理する際のパスワード要件。
- ID ソースが の場合はAWS Managed Microsoft AD、「」の「パスワードをリセットする際のパスワード要件 AWS Managed Microsoft AD」を参照してください。

AWS アクセスポータルにパスワードをリセットするには

1. ウェブブラウザを開き、 AWS アクセスポータルのサインインページに移動します。

   AWS アクセスポータル URL がない場合は、E メールを確認してください。 AWS アクセスポータルへの特定のサインイン URL を含む AWS IAM Identity Center への参加の招待メールが届いているはずです。または、管理者がワンタイムパスワードと AWS アクセスポータル URL を直接提供した場合もあります。この情報が見つからない場合は、管理者に連絡して送信してもらってください。

AWS アクセスポータルへのサインインの詳細については、「 ユーザーガイド」の AWS 「 アクセスポータルにサインインするAWS サインイン 」を参照してください。

2. [ユーザー名] を入力し、[次へ] を選択します。
3. [パスワード] で [パスワードを忘れた場合] を選択します。

   [ユーザー名] を入力し、提供されたイメージの文字を入力してロボットではないことを確認します。次いで、[次へ] を選択します。文字を入力できない場合は、広告ブロックソフトウェアを無効にする必要がある場合があります。
4. パスワードリセットの E メールが送信されたことを確認するメッセージが表示されます。[Continue] を選択します。
5. no-reply@signin.aws から、「パスワードのリセットがリクエストされました」という件名のメールが届きます。メールで「パスワードのリセット」を選択します。
6. 「パスワードのリセット」ページで、ユーザー名 を確認し、 AWS アクセスポータルの新しいパスワードを指定し、「新しいパスワードの設定」を選択します。
7. no-reply@signin.awsから「パスワードが更新されました」という件名のメールが届きます。

> **Note**
>
> 管理者は、パスワードのリセット手順を記載したメールを送信するか、ワンタイムパスワードを生成してユーザーと共有することで、パスワードをリセットできます。管理者の方は、「エンドユーザーの IAM Identity Center ユーザーパスワードをリセットします。」を参照してください。

AWS CLI または AWS SDKs

IAM Identity Center のユーザー認証情報で AWS Command Line Interface または AWS Software Development Kit (SDKsを使用して、プログラムで AWS サービスにアクセスできます。このトピックでは、IAM Identity Center のユーザーの一時的な認証情報を取得する方法について説明します。

AWS アクセスポータルは、IAM Identity Center ユーザーに AWS アカウント およびクラウドアプリケーションへのシングルサインオンアクセスを提供します。IAM Identity Center ユーザーとして AWS アクセスポータルにサインインすると、一時的な認証情報を取得できます。その後、 AWS CLI

または AWS SDKs で IAM Identity Center ユーザー認証情報とも呼ばれる認証情報を使用して、 のリソースにアクセスできます AWS アカウント。

を使用して AWS プログラムでサービス AWS CLI にアクセスする場合は、このトピックの手順を使用して へのアクセスを開始できます AWS CLI。の詳細については AWS CLI、「 AWS Command Line Interface ユーザーガイド」を参照してください。

AWS SDKs を使用してプログラムで AWS サービスにアクセスする場合、このトピックの手順に従って AWS SDKs。 AWS SDKsAWS SDKs」を参照してください。

> **Note**
>
> IAM Identity Center のユーザーは「IAM ユーザー」とは異なります。IAM ユーザーには、AWS リソースへの長期的な認証情報が付与されます。IAM Identity Center のユーザーには一時的な認証情報が付与されます。これらの認証情報はサインインするたびに生成される AWS アカウント ため、 にアクセスするためのセキュリティのベストプラクティスとして一時的な認証情報を使用することをお勧めします。

前提条件

IAM Identity Center ユーザーの一時認証情報を取得するには、以下が必要です。

- IAM Identity Center ユーザー — このユーザーとして AWS アクセスポータルにサインインします。ユーザーまたは管理者がこのユーザーを作成できます。IAM Identity Center を有効化して IAM Identity Center ユーザーを作成する方法については、IAM アイデンティティセンターで一般的なタスクを開始する を参照してください。
- へのユーザーアクセス AWS アカウント – IAM Identity Center ユーザーに一時的な認証情報を取得するアクセス許可を付与するには、ユーザーまたは管理者が IAM Identity Center ユーザーをアクセス許可セット に割り当てる必要があります。権限セットは IAM Identity Center に保存され、IAM Identity Center ユーザーが AWS アカウントに対して持つアクセスレベルを定義します。管理者が IAM Identity Center ユーザーを作成した場合は、このアクセス権を追加してもらうよう依頼してください。詳細については、「へのユーザーアクセスを割り当てる AWS アカウント」を参照してください。
- AWS CLI インストール済み – 一時的な認証情報を使用するには、 をインストールする必要があります AWS CLI。手順については、「AWS CLI ユーザーガイド」の「AWS CLIの最新バージョンのインストールまたは更新」を参照してください。

考慮事項

IAM Identity Center ユーザーの一時的な認証情報を取得する手順を完了する前に、以下の考慮事項に注意してください。

- IAM Identity Center は IAM ロールを作成する ー IAM Identity Center のユーザーを権限セットに割り当てると、IAM Identity Center はその権限セットから対応する IAM ロールを作成します。アクセス許可セットによって作成された IAM ロールは、 で作成された IAM ロールと以下の点 AWS Identity and Access Management で異なります。
  - IAM Identity Center は、権限セットによって作成されたロールを所有し、保護します。IAM Identity Center のみがこれらのロールを変更できます。
  - IAM Identity Center のユーザーのみが、割り当てられた権限セットに対応するロールを引き受けることができます。権限セットへのアクセスを IAM ユーザー、IAM フェデレーティッドユーザー、またはサービスアカウントに割り当てることはできません。
  - これらのロールのロール信頼ポリシーを変更して IAM Identity Center 外の「プリンシパル」へのアクセスを許可することはできません。

  IAM で一時的な認証情報を取得する方法については、「AWS Identity and Access Management ユーザーガイド」の「AWS CLIで一時的なセキュリティ認証情報を使用する」を参照してください。
- アクセス権限セットのセッション期間を設定できます – AWS アクセスポータルにサインインすると、IAM Identity Center ユーザーに割り当てられているアクセス権限セットが使用可能なロールとして表示されます。IAM Identity Center は、このロール用に別のセッションを作成します。このセッションは、権限セットに設定されているセッション時間に応じて 1 時間から 12 時間まで可能です。デフォルトでは、セッションの有効期間は 1 時間です。詳細については、「セッション期間の設定」を参照してください。

一時的な認証情報の取得と更新

IAM Identity Center ユーザーの一時認証情報は、自動または手動で取得および更新できます。

トピック

- 認証情報の自動更新 (推奨)
- 認証情報の手動更新

認証情報の自動更新 (推奨)

認証情報の自動更新は、Open IdConnect Center (OIDC) デバイスコード認証標準を使用します。この方法では、 AWS CLIの `aws configure sso` コマンドを使用して直接アクセスを開始します。このコマンドを使用して、任意の に対して割り当てられているアクセス許可セットに関連付けられているすべてのロールに自動的にアクセスできます AWS アカウント。

IAM Identity Center ユーザー用に作成されたロールにアクセスするには、 `aws configure sso` コマンドを実行し、ブラウザウィンドウ AWS CLI から を承認します。アクティブな AWS アクセスポータルセッションがある限り、 は一時的な認証情報 AWS CLI を自動的に取得し、認証情報を自動的に更新します。

詳細については、AWS Command Line Interface ユーザーガイドの「`aws configure sso wizard` を使用したプロフィール設定」を参照してください。

自動的に更新される一時的な認証情報を取得するには

1. 管理者から提供された特定のサインイン URL を使用して、 AWS アクセスポータルにサインインします。IAM Identity Center ユーザーを作成した場合は、サインイン URL を含む招待 AWS メールを送信します。詳細については、「 サインインユーザーガイド」の AWS 「 アクセスポータルへのAWS サインイン」を参照してください。
2. アカウント タブで、認証情報を取得する AWS アカウント を見つけます。アカウントを選択すると、そのアカウントに関連付けられているアカウント名、アカウント ID、および E メールアドレスが表示されます。

   > **Note**
   >
   > AWS アカウント が一覧表示されていない場合は、そのアカウントの権限セットに割り当てられていない可能性があります。この場合は、管理者に連絡して、このアクセス権を追加してもらうよう依頼してください。詳細については、「へのユーザーアクセスを割り当てる AWS アカウント」を参照してください。

3. アカウントの下に、IAM Identity Center ユーザーに割り当てられている権限セットの名前が使用可能なロールとして表示されます。例えば、IAM Identity Center ユーザーがアカウントのPowerUserAccessアクセス許可セットに割り当てられている場合、ロールは AWS アクセスポータルに として表示されますPowerUserAccess。
4. ロール名の横にあるオプションに応じて、アクセスキーを選択するか、コマンドラインまたはプログラムによるアクセスを選択します。

5. 「認証情報の取得」ダイアログボックスで、 をインストールしたオペレーティングシステムに応じてPowerShell、macOS と Linux 、Windows 、または を選択します AWS CLI。
6. 「AWS IAM Identity Center の認証情報 (推奨)」に、`SSO Start URL` と `SSO Region` が表示されます。これらの値は、IAM Identity Center で有効化されたプロファイルおよび `sso-session` を AWS CLIに対して設定する必要があります。この設定を完了するには、「AWS Command Line Interface ユーザーガイド」の「`aws configure sso wizard` でプロファイルを設定」の指示に従います。

認証情報の有効期限が切れ AWS アカウント るまで、 AWS CLI 必要に応じて を に引き続き使用します。

認証情報の手動更新

手動認証情報更新方法を使用して、特定の の特定のアクセス許可セットに関連付けられているロールの一時的な認証情報を取得できます AWS アカウント。そのためには、一時的な認証情報に必要なコマンドをコピーして貼り付けます。この方法では、一時的な認証情報を手動で更新する必要があります。

一時的な認証情報の有効期限が切れるまで AWS CLI コマンドを実行できます。

手動で更新する認証情報を取得するには

1. 管理者から提供された特定のサインイン URL を使用して、 AWS アクセスポータルにサインインします。IAM Identity Center ユーザーを作成した場合は、サインイン URL を含む招待 AWS メールを送信します。詳細については、「 サインインユーザーガイド」の AWS 「 アクセスポータルへのAWS サインイン」を参照してください。
2. アカウント タブ AWS アカウント で、アクセス認証情報を取得する を見つけ、展開して IAM ロール名 (管理者 など) を表示します。IAM ロール名の横にあるオプションに応じて、アクセスキーを選択するか、コマンドラインまたはプログラムによるアクセスを選択します。

> **Note**
>
> AWS アカウント が一覧表示されていない場合は、そのアカウントの権限セットに割り当てられていない可能性があります。この場合は、管理者に連絡して、このアクセス権を追加してもらうよう依頼してください。詳細については、「へのユーザーアクセスを割り当てる AWS アカウント」を参照してください。

3. 「認証情報の取得」ダイアログボックスで、 をインストールしたオペレーティングシステムに応じて、MacOS と Linux PowerShell、Windows 、または を選択します AWS CLI。
4. 次のいずれかのオプションを選択します。

   - オプション 1: AWS 環境変数を設定する

     このオプションを選択すると、`credentials`ファイルおよび`config`ファイル内の設定を含むすべての認証情報設定が上書きされます。詳細については、「AWS CLI ユーザガイド」の「AWS CLIを設定するための環境変数」を参照してください。

     このオプションを使用するには、コマンドをクリップボードにコピーし、コマンドを AWS CLI ターミナルウィンドウに貼り付け、Enter キーを押して必要な環境変数を設定します。

   - オプション 2: AWS 認証情報ファイルにプロファイルを追加する

     このオプションを選択すると、さまざまな認証情報を使用してコマンドを実行できます。

     このオプションを使用するには、コマンドをクリップボードにコピーし、コマンドを共有 AWS `credentials`ファイルに貼り付けて、新しい名前付きプロファイルを設定します。詳細については、「AWS SDK とツールのリファレンスガイド」の「共有設定ファイルおよび認証情報ファイル」を参照してください。この認証情報を使用するには、 AWS CLI コマンドで`--profile`オプションを指定します。このことは、この同じ認証情報ファイルを使用するすべての環境にも当てはまります。

   - オプション 3: AWS サービスクライアントで個々の値を使用する

     AWS サービスクライアントから AWS リソースにアクセスするには、このオプションを選択します。詳細については、「 で構築するツール AWS」を参照してください。

     このオプションを使用するには、値をクリップボードにコピーし、その値をコードに貼り付け、SDK の適切な変数に割り当てます。詳細については、お使いの SDK API 固有のドキュメントを参照してください。

AWS Management Console 送信先へのショートカットリンクの作成

AWS アクセスポータルで作成されたショートカットリンクにより、IAM Identity Center ユーザーは、 内の特定の宛先 AWS Management Console、特定のアクセス許可セット、および特定の に移動します AWS アカウント。

ショートカットリンクは、ユーザーと共同作業者の時間を節約します。 AWS アクセスポータルを含む複数のページを介して で目的の宛先 URL AWS Management Console (Amazon S3 バケットインスタンスページなど) に移動する代わりに、ショートカットリンクを使用して同じ宛先に自動的にアクセスできます。

ショートカットリンクの送信先オプション

ショートカットリンクには 3 つの送信先オプションがあり、優先度別にリストされています。

- (オプション) ショートカットリンクで AWS Management Console 指定された の送信先 URL。例えば、Amazon S3 バケットインスタンスページなどです。
- (オプション) 該当するアクセス許可セットの管理者設定のリレーステート URL。リレーステートの設定の詳細については、「」を参照してくださいリレーステートの設定。
- AWS Management Console ホーム 指定しない場合のデフォルトの送信先。

> **Note**
>
> 送信先への自動ナビゲーションは、IAM Identity Center で認証され、 AWS アカウントと送信先 URL に必要なアクセス許可セットが割り当てられている場合にのみ成功します。

AWS アクセスポータルには、共有可能なショートカットリンクの作成に役立つショートカットの作成ボタンが含まれています。送信先 URL (前のリストの最初のオプション) を指定する場合は、URL をクリップボードにコピーして共有できます。

AWS アクセスポータルでショートカットリンクを作成する

1. AWS アクセスポータルにサインインしたら、アカウントタブを選択し、ショートカットの作成ボタンを選択します。
2. ダイアログボックスで、次の操作を行います。

    a. アカウント ID またはアカウント名 AWS アカウント を使用して を選択します。入力すると、ドロップダウンメニューに、アクセス可能な一致するアカウント IDsと名前が表示されます。アクセス可能なアカウントのみを選択できます。

    b. 必要に応じて、ドロップダウンリストから IAM ロールを選択します。これらは、選択したアカウントに割り当てられたアクセス許可セットです。ロールの選択を省略すると、ショートカットリンクを使用するときに、ユーザーは選択したアカウントに割り当てられたロールを選択するように求められます。

> **Note**
>
> ショートカットリンクを使用して新しいアクセスを許可することはできません。ショートカットリンクは、ユーザーに既に割り当てられているアクセス許可セットでのみ機能します。ユーザーにアカウントと送信先 URL に必要なアクセス許可セットが割り当てられていない場合、アクセスは拒否されます。

c. 必要に応じて、 AWS アクセスポータルの送信先 URL を入力します。URL の入力を省略すると、前述のショートカットリンクの送信先オプションに基づいて、ショートカットリンクの使用時に送信先が自動的に決定されます。

d. ショートカットリンクは、入力に基づいてダイアログボックスの下部に生成されます。URL のコピーボタンを選択します。コピーしたショートカットリンクでブックマークを作成するか、同じアクセス許可セットまたは別の十分なアクセス許可セットを持つ同じアカウントにアクセスできる共同作業者と共有できるようになりました。

URL エンコーディングを使用した安全な AWS Management Console ショートカットリンクの構築

アカウント ID、アクセス許可セット名、送信先 URL など、URL のすべてのパラメータ値は、URL エンコードされている必要があります。

ショートカットリンクは、 アクセスポータル URL AWS を次のパスで拡張します。

```
/#/console?
account_id=[account_ID]&role_name=[permission_set_name]&destination=[destination
```

クラシック AWS パーティションの完全な URL は、次のパターンに従います。

```
https://[your_subdomain].awsapps.com/start/#/console?
account_id=[account_ID]&role_name=[permission_set_name]&destination=[destination
```

アクセス`S3FullAccess`許可セット`123456789012`を使用してユーザーにサインインし、S3 コンソールのホームページに移動するショートカットリンクの例を次に示します。

- `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`

MFA 用デバイスの登録

AWS アクセスポータルで次の手順を使用して、新しいデバイスを多要素認証 (MFA) に登録します。

> **Note**
>
> この手順を開始する前に、まず適切な認証システムアプリケーションをデバイスにダウンロードすることをお勧めします。MFA デバイスに使用できるアプリケーションの一覧については、「仮想認証アプリ」を参照してください。

MFA を使用するデバイスを登録するには

1. AWS アクセスポータルにサインインします。詳細については、「AWS アクセスポータルにサインインする」を参照してください。
2. ページの右上近くにある [MFA devices] (MFA デバイス) をクリックします。
3. [Multi-factor authentication (MFA) devices] (多要素認証 (MFA) デバイス) ページで、[Register device] (デバイスの登録) をクリックします。

   > **Note**
   >
   > [MFA デバイスの登録] オプションがグレーアウトしている場合は、管理者に連絡してデバイスの登録をサポートしてもらう必要があります。

4. [MFA デバイスの登録] ページで、次の MFA デバイスタイプを選択し、指示に従います。

   - 認証システムアプリケーション

     1. [Set up the authenticator app] (認証システムアプリケーションの設定) ページで、QR コードのグラフィックを含む新しい MFA デバイスの設定情報を表示します。この図は、QR コードをサポートしていないデバイスの手動入力に使用できるシークレットキーを表しています。
     2. 物理的に MFA デバイスを使用して、次の操作を行います。

a. 互換性のある MFA 認証システムアプリケーションを開きます。MFA デバイスで使用できるテスト済みアプリケーションのリストについては、「仮想認証アプリ」を参照してください。MFA アプリケーションが複数のアカウント (複数の MFA デバイス) をサポートしている場合は、新しいアカウント (新しい MFA デバイス) を作成するオプションを選択します。

b. MFA アプリケーションが QR コードをサポートしているかどうかを判断し、[Set up the authenticator app] (認証アプリケーションの設定) ページで以下のいずれかの操作を行います。

i. [Show QR code] (QR コードの表示) を選択し、アプリケーションを使用して QR コードをスキャンします。例えば、カメラアイコンまたは スキャンコード に似たオプションを選択します。次に、デバイスのカメラでコードをスキャンします。

ii. [show secret key] (シークレットキーを表示する) をクリックし、そのシークレットキーを MFA アプリケーションに入力します。

> **Important**
>
> MFA デバイスを IAM Identity Center に設定する際には、QR コードやシークレットキーのコピーを 安全な場所に保存することをお勧めします。これは、携帯電話を紛失した場合や、MFA 認証システムアプリケーションを再インストールしなければならない場合に役立ちます。いずれの場合も、すぐにアプリケーションを再設定して同じ MFA 設定を使用することができます。

3. [Set up the authenticator app] (認証システムアプリケーションをセットアップする) ページで、[Authenticator code] (認証コード) で、物理的な MFA デバイスに現在表示されているワンタイムパスワードを入力します。

> **Important**
>
> コードを生成したら、即時にリクエストを送信します。コードを生成した後にリクエストを送信するまで時間がかかりすぎる場合、MFA デバイスは ユーザーとは正常に関連付けられますが、その MFA デバイスは同期しません。これは、タイムベースドワンタイムパスワード (TOTP) の有効期間が短いために起こります。その場合は、デバイスの再同期ができます。

4. MFA の割り当てを選択します。MFA デバイスはワンタイムパスワードの生成を開始でき、で使用できるようになりました AWS。

- セキュリティキーと内蔵認証システム
  1. [ユーザーのセキュリティキーの登録] ページでは、お使いのブラウザやプラットフォームの指示に従ってください。

     > **Note**
     >
     > エクスペリエンスはブラウザまたはプラットフォームによって異なります。デバイスが正常に登録されると、登録したデバイスに識別しやすい表示名を付けるオプションが表示されます。変更する場合は、[名前の変更] を選択し、新しい名前を入力してから [保存] を選択します。

AWS アクセスポータル URL のカスタマイズ

デフォルトでは、次の形式の URL を使用して AWS アクセスポータルにアクセスできます: `d-xxxxxxxxxx.awsapps.com/start`。プラグインは次のようにカスタマイズできます: `your_subdomain.awsapps.com/start`

> **Important**
>
> AWS アクセスポータル URL を変更した場合、後で編集することはできません。

URL をカスタマイズするには

1. https://console.aws.amazon.com/singlesignon/ で AWS IAM Identity Center コンソールを開きます。
2. IAM Identity Center コンソールで、ナビゲーションペインのダッシュボードを選択し、設定の概要セクションを見つけます。
3. AWS アクセスポータル URL の下にあるカスタマイズボタンを選択します。

   > **Note**
   >
   > カスタマイズボタンが表示されない場合は、 AWS アクセスポータルが既にカスタマイズされていることを意味します。 AWS アクセスポータル URL のカスタマイズは 1 回限りのオペレーションであり、元に戻すことはできません。

4. 目的のサブドメイン名を入力し、保存 を選択します。

これで、カスタマイズされた URL を使用して AWS アクセスポータルから AWS コンソールにサインインできます。

Identity Center ユーザー用の多要素認証

多要素認証 (MFA) は、デフォルトの認証メカニズムであるユーザー名とパスワードに加えて、さらに保護レイヤーを追加するシンプルで安全な方法です。

管理者が MFA を有効にした場合、ユーザーは次の 2 つの要素で AWS アクセスポータルにサインインする必要があります。

- ユーザー名とパスワード。これは最初の要素であり、ユーザーが知っていることです。
- コード、セキュリティキー、または生体認証のいずれか。これはもう 1 つの要素で、ユーザーが所有している (所有) または存在している (生体認証) ものです。第 2 の要素は、モバイルデバイスから生成された認証コード、コンピューターに接続されたセキュリティキー、またはユーザーの生体認証のスキャンのいずれかです。

これらの複数の要素を組み合わせることで、有効な MFA 課題が完了しない限り、AWS リソースへの不正アクセスを防ぐことができ、セキュリティが向上します。

各ユーザーは、モバイルデバイスまたはタブレットにインストールされるワンタイムパスワード認証アプリケーションである仮想認証アプリを最大 2 つと、組み込みの認証システムとセキュリティキーを含む 6 つの FIDO 認証システムを合計 8 台の MFA デバイスに登録できます。IAM Identity Center で使用可能な MFA タイプ の詳細を確認してください。

> **Important**
>
> セキュリティのベストプラクティスとして、MFA を有効化することを強くお勧めします。

トピック

- IAM Identity Center で使用可能な MFA タイプ
- MFA を設定
- IAM Identity Center で MFA デバイスを管理

IAM Identity Center で使用可能な MFA タイプ

多要素認証 (MFA) は、ユーザーのセキュリティを強化するためのシンプルで効果的なメカニズムです。ユーザーの最初の要素であるパスワードは、ユーザーが記憶する秘密であり、ナレッジファクターとも呼ばれます。その他の要素としては、所有要素 (セキュリティキーなど、所有しているもの) や継承要素(生体認証のスキャンなど、ユーザーが持っているもの) があります。MFA を設定して、アカウントのセキュリティをさらに強化することを強くお勧めします。

IAM Identity Center MFA は、以下のデバイスタイプをサポートします。すべての MFA タイプは、ブラウザベースのコンソールを通じたアクセスと、AWS CLI IAM Identity Center による v2 の使用の両方でサポートされています。

- FIDO2 認証機能 は、組み込みの認証機能とセキュリティキーを含みます。
- 仮想認証アプリ
- RADIUS MFA 独自の実装は AWS Managed Microsoft AD を介して接続されます。

ユーザーは、最大 2 つの仮想認証アプリと 6 つの FIDO 認証機能を含む最大8 台の MFA デバイスを 1 つのアカウントに登録できます。また、ユーザーがサインインするたびに MFA を必須にしたり、サインインするたびに MFA を必須にすることのない信頼されたデバイスを有効にするように、MFA 有効化設定を構成することもできます。ユーザーの MFA タイプを設定する方法の詳細については、「MFA タイプの選択 」と「MFA デバイス強制の設定」を参照してください。

FIDO2 認証機能

FIDO2 は CTAP2 と WebAuthn を含む標準であり、パブリックキー暗号に基づいています。FIDO 認証情報は、認証情報が作成された Web サイト (AWS など) 固有のものであるため、フィッシング詐欺に対して強固です。

AWS は、FIDO 認証システムの最も一般的なフォームの要素は、組み込みの認証アプリシステムとセキュリティキーの 2 つです。FIDO 認証機能の最も一般的なタイプの詳細については、以下を参照してください。

トピック

- 組み込みの認証機能
- セキュリティキー
- パスワードマネージャー、パスキープロバイダー、その他の FIDO 認証機能

組み込みの認証機能

MacBook の TouchID や、Windows Hello 対応のカメラなどの多数のコンピューターや携帯電話は組み込みの認証アプリシステムを装備しています。デバイスに FIDO 互換の組み込みの認証アプリがある場合は、指紋、顔、またはデバイスの PIN を 2 つ目の要素として使用できます。

セキュリティキー

セキュリティキーは FIDO 互換の外部ハードウェア認証機能です。ご購入の上 USB、BLE、または NFC 経由でデバイスに接続できます。MFA を要求されたら、キーのセンサーでジェスチャーを完了するだけです。セキュリティキーの例としては YubiKeys や Feitian キーがあり、最も一般的なセキュリティキーはデバイス向けの FIDO 認証情報を作成します。互換性のあるFIDO 認定のセキュリティキーの全リストについては、「FIDO 認定製品」 をご覧ください。

パスワードマネージャー、パスキープロバイダー、その他の FIDO 認証機能

複数のサードパーティプロバイダーが、パスワードマネージャー、FIDO モードのスマートカード、その他のフォームの要素の機能として、モバイルアプリケーションの FIDO 認証をサポートしています。これらの FIDO 互換デバイスは IAM Identity Center で動作しますが、このオプションを MFA で有効にする前に FIDO 認証機能をご自身でテストすることをお勧めします。

> **Note**
>
> FIDO 認証機能の中には、パスキーと呼ばれる検出可能な FIDO 認証情報を作成できるものもあります。パスキーは、パスキーを作成したデバイスにバインドされている場合もあれば、同期可能でクラウドにバックアップされている場合もあります。例えば、サポートされている Macbook で Apple Touch ID を使ってパスキーを登録し、ログイン時に画面に表示される指示に従って iCloud のパスキーで Google Chrome を使って Windows ラップトップからサイトにログインできます。どのデバイスが同期可能なパスキーをサポートしているか、および運用システムとブラウザ間の現在のパスキーの相互運用性をサポートしているかについての詳細は、FIDO Alliance And World Wide Web Consortium (W3C) が管理するリソースである passkeys.dev の デバイスサポート を参照してください。

仮想認証アプリ

認証アプリは、基本的にワンタイムパスワード (OTP) ベースのサードパーティー認証機能を備えています。モバイルデバイスやタブレットにインストールされた認証アプリケーションを、許可された MFA デバイスとして使用することができます。サードパーティー認証アプリケーションは、6 桁の

認証コードを生成できる標準ベースのタイムベースドワンタイムパスワード (TOTP) アルゴリズムである RFC 6238 に準拠している必要があります。

MFA を求めるプロンプトが表示されたら、ユーザーは認証アプリから有効なコードを入力ボックスに入力する必要があります。ユーザーに割り当てられた各 MFA デバイスは一意であることが必要です。1 人の ユーザーに対して 2 つの認証アプリを登録することができます。

テスト済みの認証アプリ

TOTP 準拠のアプリケーションはどれも IAM Identity Center MFA と連携して動作します。以下の有名なサードパーティの認証アプリから選択できます。

オペレーティングシステム	テスト済みの認証アプリ
Android	Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator
iOS	Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator

RADIUS MFA

リモート認証ダイヤルインユーザー サービス (RADIUS) は、業界標準のクライアント/サーバープロトコルであり、ユーザーをネットワークサービスに接続するための認証、認可、アカウント管理を行うことができます。AWS Directory Service には、MFA ソリューションを実装した RADIUS サーバーに接続する RADIUS クライアントが付属しています。詳細については、「AWS Managed Microsoft AD の多要素認証を有効にする」 を参照してください。

ユーザーポータルへのサインインには、IAM Identity Center で RADIUS MFA または MFA のいずれかを使用できますが、両方を使用することはできません。IAM Identity Center での MFA は、ポータルへのアクセスに AWS ネイティブの二要素認証が必要な場合に、RADIUS MFA の代わりに使用されます。

IAM Identity Center で MFA を有効にすると、ユーザーは AWS アクセスポータルにサインインするために MFA デバイスが必要になります。これまで RADIUS MFA を使用していた場合、IAM Identity Center で MFA を有効にすると、AWS アクセスポータルにサインインしたユーザーの RADIUS MFA が効果的に上書きされます。ただし、RADIUS MFA は、Amazon WorkDocs など、AWS Directory Service と連携する他のすべてのアプリケーションにサインインする際に、ユーザーに課題を与え続けます。

IAM Identity Center コンソールで MFA が 無効 になっていて、AWS Directory Service で RADIUS MFA を設定している場合、RADIUS MFA が AWS アクセスポータルのサインインを管理します。これは、MFA が無効になっている場合、IAM Identity Center は RADIUS MFA 設定にフォールバックすることを意味します。

MFA を設定

以下のトピックでは、IAM Identity Center で MFA デバイスを設定するための手順を説明しています。

トピック

IAM Identity Center で MFA を有効にする前に考慮すること

MFA を有効化する前に、次の情報を考慮してください。

- ユーザーには、有効なすべての MFA タイプについて、複数のバックアップ認証の登録を推奨します。これにより、MFA デバイスが壊れたり、置き忘れたりした場合に、ユーザーがアクセスできなくなることを防げます。
- ユーザーが E メールにアクセスするために AWS アクセスポータルにサインインする必要がある場合は、[E メールで送信されたワンタイムパスワードの提供を要求する]のオプションを選択しないでください。例えば、ユーザーは AWS アクセスポータルを Microsoft 365 使用して E メールを読む可能性があります。この場合、ユーザーは認証コードを取得することができず、AWS アクセスポータルにサインインすることができなくなります。詳細については、「MFA デバイス強制の設定」を参照してください。
- AWS Directory Service で設定した RADIUS MFA を既に使用している場合は、IAM Identity Center 内で MFA を有効化する必要はありません。IAM Identity Center の MFA は、IAM Identity Center Microsoft Active Directory ユーザーにとって、RADIUS MFA の代替となるものです。詳細については、「RADIUS MFA」を参照してください。

- ID ソースが IAM Identity Center の ID ストア、AWS Managed Microsoft AD または AD Connector で設定されている場合、IAM Identity Center の MFA 機能を使用できます。IAM Identity Center の MFA は、現在、外部 ID プロバイダー による使用はサポートされていません。

IAM Identity Center で MFA を有効化する

多要素認証 (MFA) を有効にすることで、AWS アクセスポータル、IAM Identity Center の統合アプリ、および 多要素認証 (MFA)を有効にすることで AWS CLI へのアクセスの安全性を強化することができます。

トピック

- ユーザーに MFA を求める
- IAM Identity Center ディレクトリの MFA を無効化

ユーザーに MFA を求める

以下の手順で、 IAM Identity Center コンソールを使って MFA を有効化します。開始する前に、IAM Identity Center で使用可能な MFA タイプ を理解することをお勧めします。

> **Note**
>
> 外部の IdP を使用している場合は、[多要素認証] の項目は表示されません。MFA 設定を IAM Identity Center が管理するのではなく、外部の IdP が管理します。

MFA を有効にするには

1. IAM Identity Center コンソール を開きます。
2. 左のナビゲーションペインの [設定] を選択します。
3. 「設定」 ページで、「認証」タブを選択します。
4. [多要素認証] セクションで、[設定] を選択します。
5. [多要素認証を設定] ページの [MFA のプロンプトをユーザーに表示] で、ビジネスに必要なセキュリティのレベルに基づいて、次の認証モードのいずれかを選択します。
   - サインインコンテキストが変更された場合のみ (context-aware)

このモード (デフォルト) では、IAM Identity Center はサインイン中にデバイスを信頼するオプションをユーザーに提供します。ユーザーがデバイスを信頼することを表明すると、IAM Identity Center はユーザーに MFA の入力を一度要求し、ユーザーが次にサインインする際のサインインコンテキスト (デバイス、ブラウザ、場所など) を分析します。後続のサインインでは、IAM Identity Center は、ユーザーが以前に信頼されたコンテキストでサインインしているかどうかを判断します。ユーザーのサインインコンテキストが変更されると、IAM Identity Center はユーザーに E メールアドレスとパスワードの認証情報に加えて MFA の入力を求めます。

このモードでは、職場から頻繁にサインインするユーザーが使いやすく、サインインのたびに MFA を完了する必要はありません。サインインコンテキストが変更された場合にのみ MFA を要求されます。

- サインインごと (常時オン)

  このモードでは、 IAM Identity Center は、登録された MFA デバイスを持つユーザーがサインインごとにプロンプトを表示することを要求します。このモードは、ユーザーが AWS アクセスポータルにサインインするごとに MFA を完了することを、組織ポリシーまたはコンプライアンスポリシーで定めている場合に使用します。例えば、PCI DSS は、高リスクの支払取引をサポートするアプリケーションにアクセスする際のすべてのサインイン時に MFA を使用することを強く推奨しています。

- なし (無効)

  このモードでは、すべてのユーザーが標準のユーザー名とパスワードのみでサインインします。このオプションを選択すると、IAM Identity Center MFA を無効にします。

> **Note**
>
> 既に AWS Directory Service で RADIUS MFA を使用しており、今後もデフォルトの MFA タイプとして使用したい場合は、認証モードを無効のままにしておくと、IAM Identity Center の MFA 機能をバイパスできます。Disabled (無効) モードから Context-aware または Always-on モードに変更すると、既存の RADIUS MFA 設定が上書きされます。詳細については、「RADIUS MFA」を参照してください。

6. [変更の保存] を選択します。

関連トピック

- MFA タイプの選択

- MFA デバイス強制の設定
- ユーザーが自分の MFA デバイスを登録できるようにする

IAM Identity Center ディレクトリの MFA を無効化

IAM Identity Center ディレクトリの多要素認証 (MFA) を無効にすると、ユーザーは標準のユーザー名とパスワードのみでサインインできるようになります。ユーザーの Identity Center ディレクトリでは MFA が無効になっていますが、ユーザー詳細で MFA デバイスを管理することはできません。また、Identity Center ディレクトリのユーザーは AWS アクセスポータルから MFA デバイスを管理できません。

IAM Identity Center ディレクトリの MFA を無効化するには

> **Important**
>
> このセクションの手順は AWS IAM Identity Center に適用されます。これらは AWS Identity and Access Management (IAM) には適用されません。IAM Identity Center ユーザー、グループ、およびユーザー認証情報は、IAM ユーザー、グループ、IAM ユーザー認証情報とは異なります。IAM ユーザーの MFA を無効化する手順をお探しの場合は、AWS Identity and Access Managementユーザーガイドの「MFA デバイスの無効化」を参照してください。

1. IAM Identity Center コンソール を開きます。
2. 左のナビゲーションペインの [設定] を選択します。
3. 「設定」 ページで、「認証」タブを選択します。
4. [多要素認証] セクションで、[設定] を選択します。
5. 「多要素認証を設定」ページの「MFA のプロンプトをユーザーに表示」セクションで、「なし (無効)」のラジオボタンを選択します。
6. [変更の保存] を選択します。

MFA タイプの選択

以下の手順で、AWS アクセスポータルで MFA を要求されたときに、ユーザーが認証できるデバイスタイプを選択します。

ユーザーの MFA タイプを設定するには

1. IAM Identity Center コンソール を開きます。
2. 左のナビゲーションペインの [設定] を選択します。
3. 「設定」 ページで、「認証」タブを選択します。
4. [多要素認証] セクションで、[設定] を選択します。
5. [多要素認証を設定] ページでは、[ユーザーはこれらの MFA タイプで認証できます] で、ビジネスニーズに応じて次のいずれかの MFA タイプを選択します。詳細については、「IAM Identity Center で使用可能な MFA タイプ」を参照してください。
   - FIDO2 認証機能 (組み込みの認証機能とセキュリティキーを含む)
   - 仮想認証アプリ
6. [変更の保存] を選択します。

MFA デバイス強制の設定

以下の手順で、ユーザーが AWS アクセスポータルにサインインする際に、登録済みの MFA デバイスが必要かどうかを判断します。

ユーザーの MFA デバイスの強制を設定するには

1. IAM Identity Center コンソール を開きます。
2. 左のナビゲーションペインの [設定] を選択します。
3. 「設定」 ページで、「認証」タブを選択します。
4. [多要素認証] セクションで、[設定] を選択します。
5. [多要素認証の設定] ページでは、[ユーザーがまだ登録された MFA デバイスを持っていない場合] で、ビジネスニーズに応じて次のいずれかの選択肢を選択します。
   - サインイン時に MFA デバイスの登録を必須とする

     これは、IAM Identity Center の MFA を初めて設定するときのデフォルト設定です。このオプションは、まだ登録済みの MFA デバイスを持っていないユーザーに対して、パスワード認証に成功した後のサインイン時にデバイスの自己登録を要求する場合に使用します。これにより、ユーザーに認証デバイスを個別に登録したり、配信する必要がなく、組織内の AWS 環境を MFA で保護することができます。自己登録の際、ユーザーは事前に登録した IAM Identity Center で使用可能な MFA タイプ の中から任意のデバイスを登録することができます。登録

完了後、ユーザーは新しく登録した MFA デバイスに親しみのある名前を付けることができ、その後、IAM Identity Center はユーザーを元の場所にリダイレクトします。ユーザーのデバイスが紛失または盗難にあった場合、そのデバイスをユーザーのアカウントから削除するだけで、IAM Identity Center は次回のサインイン時に新しいデバイスを自己登録することが必須となります。

- E メールで送られてくるワンタイムパスワードを入力してサインインすることを必須とする

  確認コードをユーザーに E メールで送信したい場合は、このオプションを使用します。E メールは特定のデバイスに限定されないため、このオプションは業界標準の多要素認証の基準を満たしません。ですが、パスワードだけを使用するよりもセキュリティが向上します。E メール認証は、ユーザーが MFA デバイスを登録していない場合にのみ求められます。Context-aware (コンテキスト認識) の認証方法が有効になっている場合、ユーザーは E メールを受信したデバイスを信頼済みとしてマークすることができます。その後、そのデバイス、ブラウザ、IP アドレスの組み合わせでログインする際に、E メールコードを確認する必要がなくなります。

  > **Note**
  >
  > IAM Identity Center 対応の ID ソースとして Active Directory を使用している場合、E メールアドレスは常に Active Directory `email` 属性に基づいて設定されます。カスタムのアクティブディレクトリ属性のマッピングは、この動作を上書きしません。

- [Block their sign-in] (サインインをブロックする)

  すべてのユーザーが AWS にサインインする前に MFA の使用を強制したい場合は、[Block Their Sign-In] (サインインをブロックする) オプションを使用します。

  > **Important**
  >
  > 認証方法に Context-aware (コンテキストアウェア) に設定されている場合、ユーザーはサインインページで [This is a trusted device] (信頼できるデバイス) チェックボックスを選択します。この場合、[Block their sign in] (サインインをブロックする) 設定を有効でも、そのユーザーには MFA の入力が求められません。これらのユーザーにプロンプトを表示させたい場合は、認証方法を Always On (常時オン) に変更してください。

- Allow them to sign in (サインインを許可する)

このオプションは、ユーザーが AWS アクセスポータルにサインインする際に、MFA デバイスを必要としないことを示します。MFA デバイスの登録を選択したユーザーは、MFA の入力を求められます。

6. [変更の保存] を選択します。

ユーザーが自分の MFA デバイスを登録できるようにする

ユーザーが MFA デバイスを自己登録できるようにする場合は、以下の手順で実施します。

ユーザーが自分の MFA デバイスを登録できるようにするには

1. IAM Identity Center コンソール を開きます。
2. 左のナビゲーションペインの [設定] を選択します。
3. 「設定」 ページで、「認証」タブを選択します。
4. [多要素認証] セクションで、[設定] を選択します。
5. [多要素認証の設定] ページで [MFA デバイスを管理できるユーザー] に [ユーザーは自分の MFA デバイスを追加および管理できる] を選択します。
6. [変更の保存] を選択します。

> **Note**
>
> ユーザーの自己登録を設定した後、手順 MFA 用デバイスの登録 のリンクをユーザーに送信することをお勧めします。このトピックでは、自分の MFA デバイスを設定する方法を説明します。

IAM Identity Center で MFA デバイスを管理

以下のトピックでは、IAM Identity Center で MFA を管理するための手順を説明しています。

トピック

- MFA デバイスを登録する
- ユーザーの MFA デバイスを管理する

MFA デバイスを登録する

以下の手順により、IAM Identity Center コンソールから特定のユーザーがアクセスするための新しい MFA デバイスを設定します。登録するには、ユーザーの MFA デバイスに物理的にアクセスできる必要があります。例えば、スマートフォンで実行される MFA デバイスを使用するユーザー用に MFA を設定する場合、登録プロセスを完了するには、スマートフォンに物理的にアクセスする必要があります。あるいは、ユーザーが自分の MFA デバイスを構成して管理できるように許可することもできます。詳細については、「ユーザーが自分の MFA デバイスを登録できるようにする」を参照してください。

MFA デバイスを登録するには

1. IAM Identity Center コンソール を開きます。
2. 左のナビゲーションペインで、[ユーザー] を選択します。リスト内でユーザーを選択します。このステップでは、ユーザーの横にあるチェックボックスをオンにしないでください。
3. [MFA デバイス] タブを選択し、[MFA デバイスの登録] を選択します。
4. [MFA デバイスの登録] ページで、次の MFA デバイスタイプを選択し、指示に従います。

   - 認証システムアプリケーション

     1. [認証システムアプリケーションの設定] ページで、IAM Identity Center は QR コードのグラフィックを含む新しい MFA デバイスの設定情報を表示します。図は、QR コードに対応していないデバイスのマニュアル入力に利用できるシークレットキーを示しています。
     2. 物理的に MFA デバイスを使用して、次の操作を行います。

        a. 互換性のある MFA 認証システムアプリケーションを開きます。MFA デバイスで使用できるテスト済みアプリケーションのリストについては、「仮想認証アプリ」を参照してください。MFA アプリケーションが複数のアカウント (複数の MFA デバイス) をサポートしている場合は、新しいアカウント (新しい MFA デバイス) を作成するオプションを選択します。

        b. MFA アプリケーションが QR コードをサポートしているかどうかを判断し、[Set up the authenticator app] (認証アプリケーションの設定) ページで以下のいずれかの操作を行います。

           i. [Show QR code] (QR コードの表示) を選択し、アプリケーションを使用して QR コードをスキャンします。例えば、カメラアイコンまたは [Scan code] (スキャンコード) に似たオプションを選択します。次に、デバイスのカメラでコードをスキャンします。

ii. [show secret key] (シークレットキーを表示する) を選択し、そのシークレットキーを MFA アプリケーションに入力します。

> **Important**
>
> MFA デバイスを IAM Identity Center に設定する際には、QR コードやシークレットキーのコピーを 安全な場所に保存することをお勧めします。これにより、割り当てられたユーザーが携帯電話を紛失したり、MFA 認証アプリケーションを再インストールしなければならない場合に役立ちます。いずれの場合も、すぐにアプリケーションを再設定して同じ MFA 設定を使用することができます。これにより、ユーザーのために IAM Identity Center で新しい MFA デバイスを作成する必要がなくなります。

3. [Set up the authenticator app] (認証アプリケーションの設定) ページで、[Authenticator code] (認証コード) で、物理的な MFA デバイスに現在表示されているワンタイムパスワードを入力します。

> **Important**
>
> コードを生成したら、即時にリクエストを送信します。コードを生成した後にリクエストを送信するまで時間がかかりすぎる場合、MFA デバイスはユーザーと正常に関連付けられます。ただし、MFA デバイスは同期しません。これは、タイムベースドワンタイムパスワード (TOTP) の有効期間が短いために起こります。その場合は、デバイスの再同期ができます。

4. [Assign MFA] (MFA の割り当て) を選択します。これで、MFA デバイスはワンタイムパスワードの生成を開始し、AWS で使用できるようになります。

- セキュリティキー

1. [Register your user's security key] (ユーザーのセキュリティキーの登録) ページでは、お使いのブラウザやプラットフォームの指示に従ってください。

> **Note**
>
> ここでの操作性は、運用システムやブラウザの違いによって異なりますので、お使いのブラウザやプラットフォームで表示される指示に従ってください。ユーザーのデバイスが正常に登録されると、登録したデバイスに識別しやすい表示名を付ける

オプションが表示されます。変更する場合は、[Rename] (名前の変更) を選択し、新しい名前を入力してから [Save] (保存) を選択します。ユーザー自身がデバイスを管理できるオプションが有効の場合、ユーザーには AWS アクセスポータルに登録した親しみのある名前が表示されます。

ユーザーの MFA デバイスを管理する

ユーザーの MFA デバイスの名前を変更または削除する場合は、以下の手順で実施します。

MFA デバイスの名前を変更するには

1. IAM Identity Center コンソール を開きます。
2. 左のナビゲーションペインで、[ユーザー] を選択します。リスト内でユーザーを選択します。このステップでは、ユーザーの横にあるチェックボックスをオンにしないでください。
3. ユーザーの詳細ページで、[MFA デバイス] タブを選択し、デバイスを選択して、[名前の変更] を選択します。
4. プロンプトが表示されたら、新しい名前を入力し、[名前の変更] を選択します。

MFA デバイスを削除するには

1. IAM Identity Center コンソール を開きます。
2. 左のナビゲーションペインで、[ユーザー] を選択します。リスト内でユーザーを選択します。
3. ユーザーの詳細ページで、[MFA デバイス] タブを選択し、デバイスを選択して、[削除] を選択します。
4. 確認のため、DELETE と入力し、[Delete] (削除) を選択します。

へのアクセスを管理する AWS アカウント

AWS IAM Identity Center は と統合されているため AWS Organizations、各アカウントを手動で設定 AWS アカウント することなく、複数の にわたるアクセス許可を一元管理できます。アクセス許可を定義し、これらのアクセス許可をワークフォースユーザーに割り当てて、特定の へのアクセスを制御できます AWS アカウント。

AWS アカウント タイプ

AWS アカウント には 2 つのタイプがあります AWS Organizations。

- 管理アカウント - 組織の作成 AWS アカウント に使用される 。
- メンバーアカウント - 組織 AWS アカウント に属する残りの 。

AWS アカウント タイプの詳細については、「 AWS Organizations ユーザーガイド」のAWS Organizations 「用語と概念」を参照してください。

IAM Identity Center の「委任管理者」としてメンバーアカウントを登録することもできます。このアカウントのユーザーは、ほとんどの IAM Identity Center 管理タスクを実行できます。詳細については、「委任された管理」を参照してください。

次の表は、タスクとアカウントタイプごとに、IAM Identity Center 管理タスクをアカウント内のユーザーが実行できるかどうかを示しています。

IAM Identity Center 管理タスク	メンバーアカウント	委任された管理者アカウント	管理アカウント
ユーザーまたはグループの読み取り (グループ自体とグループのメンバーシップの読み取り)	 はい	 はい	 はい
ユーザーまたはグループを追加、編集、削除する	 いいえ	 はい	 はい

IAM Identity Center 管理タスク	メンバーアカウント	委任された管理者アカウント	管理アカウント
ユーザーアクセスの有効化または無効化	 いいえ	 はい	 はい
受信属性を有効化、無効化、管理する	 いいえ	 はい	 はい
ID ソースの変更または管理	 いいえ	 はい	 はい
アプリケーションの作成、編集、削除を行う	 いいえ	 はい	 はい
MFA を設定	 いいえ	 はい	 はい
管理アカウントにプロビジョニングされていない権限セットを管理する	 いいえ	 はい	 はい
管理アカウントにプロビジョニングされた権限セットを管理する	 いいえ	 いいえ	 はい

IAM Identity Center 管理タスク	メンバーアカウント	委任された管理者アカウント	管理アカウント
IAM Identity Center を有効にする	 いいえ	 いいえ	 はい
IAM Identity Center 設定を削除する	 いいえ	 いいえ	 はい
管理アカウントのユーザーアクセスを有効または無効にします。	 いいえ	 いいえ	 はい
メンバーアカウントを委任管理者として登録または登録解除する	 いいえ	 いいえ	 はい

AWS アカウント アクセスの割り当て

「権限セット」を使用すると、組織内のユーザーやグループに AWS アカウントへのアクセスを割り当てる方法を簡素化することができます。権限セットは IAM Identity Center に保存され、ユーザーおよびグループが持つこの AWS アカウントに対するアクセスのレベルを定義します。1 つのアクセス許可セットを作成し、組織 AWS アカウント 内の複数の に割り当てることができます。同じユーザに複数の権限セットを割り当てることもできます。

アクセス権限セットの詳細については、「アクセス許可セットの作成、管理と削除」を参照してください。

> **Note**
>
> また、ユーザーにアプリケーションへのシングルサインオンアクセスを割り当てることもできます。詳細については、「アプリケーションへのアクセスの管理」を参照してください。

エンドユーザーエクスペリエンス

AWS アクセスポータルでは、IAM Identity Center ユーザーは、ウェブポータルを通じて、割り当てられたすべての AWS アカウント およびアプリケーションへのシングルサインオンアクセスが可能になります。 AWS アクセスポータルはAWS Management Console、 AWS リソースを管理するためのサービスコンソールのコレクションである とは異なります。

アクセス権限セットを作成すると、アクセス権限セットに指定した名前が、使用可能なロールとして AWS アクセスポータルに表示されます。ユーザーは AWS アクセスポータルにサインインし、 を選択し AWS アカウント、ロールを選択します。ロールを選択すると、 を使用して AWS サービスにアクセスしたり、一時的な認証情報 AWS Management Console を取得してプログラムで AWS サービスにアクセスしたりできます。

を開く AWS Management Console か、一時的な認証情報を取得してプログラムで にアクセスするには AWS 、ユーザーは次のステップを実行します。

1. ユーザーはブラウザウィンドウを開き、指定したサインイン URL を使用して AWS アクセスポータルに移動します。
2. ディレクトリの認証情報を使用して、 AWS アクセスポータルにサインインします。
3. 認証後、 AWS アクセスポータルページで アカウント タブを選択すると、 AWS アカウント アクセスできる のリストが表示されます。
4. 次に、ユーザーは使用する AWS アカウント を選択します。
5. の名前の下に AWS アカウント、ユーザーが割り当てられるアクセス許可セットが使用可能なロールとして表示されます。例えば、アクセスPowerUser許可セットjohn_stilesにユーザーを割り当てた場合、ロールは AWS アクセスポータルに として表示されますPowerUser/john_stiles。複数のアクセス権限セットが割り当てられている場合は、使用する ロールを選択する。ユーザーは自分のロールを選択して にアクセスできます AWS Management Console。
6. ロールに加えて、 AWS アクセスポータルのユーザーは、アクセスキー を選択して、コマンドラインまたはプログラムによるアクセス用の一時的な認証情報を取得できます。

ワークフォースユーザーに提供できる step-by-step ガイダンスについては、AWS アクセスポータルの使用「」および「」を参照してくださいAWS CLI または AWS SDKs。

アクセスの強制と制限

IAM Identity Center を有効にすると、IAM Identity Center はサービスにリンクされたロールを作成します。サービスコントロールポリシーを使用することもできます。

アクセス権の委任と強制

サービスにリンクされたロールは、 AWS サービスに直接リンクされた IAM ロールの一種です。IAM Identity Center を有効にすると、IAM Identity Center は組織 AWS アカウント 内の各 にサービスにリンクされたロールを作成できます。このロールは、IAM Identity Center が の組織 AWS アカウント 内の特定の へのシングルサインオンアクセス権を持つユーザーを委任して強制できるようにする事前定義されたアクセス許可を提供します AWS Organizations。このロールを使用するには、アカウントへのアクセス権を持つユーザーを 1 人以上割り当てる必要があります。詳細については、「サービスリンクロール」および「IAM Identity Center のサービスリンクロールの使用」を参照してください。

メンバーアカウントからのアイデンティティストアへのアクセスを制限する

IAM Identity Center で使用される Identity Store サービスの場合、メンバーアカウントにアクセスできるユーザーは、「読み取り」権限を必要とする API アクションを使用できます。メンバーアカウントは、「sso-directory」および「identitystore」ネームスペースの両方に対して「読み取り」アクションにアクセスできます。詳細については、「サービス認証リファレンス」の AWS IAM Identity Center「ディレクトリのアクション、リソース、および条件キー」および AWS「Identity Store のアクション、リソース、および条件キー」を参照してください。

メンバーアカウントのユーザーが Identity Store で API 操作を使用できないようにするには、「サービスコントロールポリシー (SCP) をアタッチ」できます。SCP は、組織のアクセス許可の管理に使用できる組織ポリシーの一種です。次の SCP の例では、メンバーアカウントのユーザーがアイデンティティストア内のあらゆる API オペレーションにアクセスできないようにします。

```
        {
            "Sid": "ExplicitlyBlockIdentityStoreAccess",
            "Effect": "Deny",
```

```
            "Action": "identitystore:*", "sso-directory:*"],
            "Resource": "*"
        }
```

> **Note**
>
> メンバーアカウントのアクセスを制限すると、IAM Identity Center 対応アプリケーションの機能が損なわれる可能性があります。

詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー (SCPs)」を参照してください。

委任された管理

委任管理により、登録済みのメンバーアカウントに割り当てられたユーザーが IAM Identity Center の大部分の管理タスクを簡単に実行できます。IAM Identity Center を有効にすると、IAM Identity Center インスタンスは AWS Organizations デフォルトで の管理アカウントに作成されます。これは当初、IAM Identity Center が組織のすべてのメンバーアカウントにわたってロールをプロビジョニング、プロビジョニング解除、更新できるようにするために設計されたものです。IAM Identity Center インスタンスは常に管理アカウントに存在する必要がありますが、IAM Identity Center の管理を のメンバーアカウントに委任することを選択できるため AWS Organizations、管理アカウント外から IAM Identity Center を管理する機能を拡張できます。

委任管理を有効にすると、次の利点があります。

- 管理アカウントへのアクセスを必要とするユーザーの数を最小限に抑え、セキュリティ上の懸念を軽減します。
- 特定の管理者が、アプリケーションや組織のメンバーアカウントにユーザーやグループを割り当てることができます。

IAM Identity Center と の連携の詳細については AWS Organizations、「」を参照してくださいへのアクセスを管理する AWS アカウント。追加情報や、委任管理の設定方法を示す企業シナリオの例を確認するには、「セキュリティブログAWS 」の「IAM Identity Center 委任管理入門」を参照してください。

トピック

ベストプラクティス

委任管理を設定する前に考慮すべきいくつかのベストプラクティスを以下に示します。

- 管理アカウントへの最小権限の付与 — 管理アカウントは特権の高いアカウントであり、最小権限の原則に従うため、管理アカウントへのアクセスをできるだけ少数のユーザーに制限することを強くお勧めします。委任管理者機能は、管理アカウントへのアクセスを必要とするユーザーの数を最小限に抑えることを目的としています。
- 管理アカウントでのみ使用する権限セットを作成 — これにより、管理アカウントにアクセスするユーザー専用の権限セットを簡単に管理できるようになり、委任された管理者アカウントによって管理される権限セットと区別しやすくなります。
- Active Directory ロケーションを検討 — IAM Identity Center のアイデンティティソースとして Active Directory を使用する予定の場合は、IAM Identity Center の委任管理者機能を有効にしたメンバーアカウント内のディレクトリを探してください。IAM Identity Center ID ソースを他のソースから Active Directory に変更するか、Active Directory から他のソースに変更する場合、そのディレクトリは IAM Identity Center 委任管理者メンバーアカウント (存在する場合) に存在する (所有されている) 必要があります。それ以外の場合は、管理アカウントに含まれている必要があります。
- 管理アカウントでのみユーザー割り当てを作成 — 委任された管理者は、管理アカウントにプロビジョニングされた権限セットを変更できません。ただし、委任管理者はグループとグループ割り当てを追加、編集、削除できます。

前提条件

アカウントを委任管理者として登録する前に、まず次の環境を展開する必要があります。

- AWS Organizations は、デフォルトの管理アカウントに加えて、少なくとも 1 つのメンバーアカウントで有効化および設定する必要があります。
- ID ソースが Active Directory に設定されている場合は、IAM Identity Center の構成可能な AD 同期機能を有効にする必要があります。

メンバーアカウントを作成する

委任管理を設定するには、まず組織のメンバーアカウントを委任管理者として登録する必要があります。そのメンバーアカウント内の十分な権限を持つユーザーは、IAM Identity Center への管理アクセス権を持ちます。メンバーアカウントが委任管理用に正常に登録されると、そのメンバーアカウントは「委任管理者アカウント」と呼ばれます。委任管理者アカウントが実行できるタスクの詳細については、AWS アカウント タイプ を参照してください。

IAM Identity Center では、一度に 1 つのメンバーアカウントのみを委任管理者として登録できます。メンバーアカウントは、管理アカウントの認証情報を使用してサインインしている場合にのみ登録できます。

AWS 組織内の特定のメンバーアカウントを委任された管理者として登録して、IAM Identity Center への管理アクセスを許可するには、以下の手順を使用します。

Important

この操作により、IAM Identity Center の管理アクセスが、このメンバーアカウントの管理者ユーザーに委任されます。この委任された管理者アカウントに対して十分な権限を持つすべてのユーザーは、以下を除くすべての IAM Identity Center 管理タスクをアカウントから実行できます。

- IAM Identity Center を有効にする
- IAM Identity Center 設定を削除する
- 管理アカウントにプロビジョニングされた権限セットの管理
- 他のメンバーアカウントを委任管理者として登録または登録解除する
- 管理アカウントでのユーザーアクセスの有効化または無効化

委任管理者はグループメンバーシップを編集できます。

メンバーアカウントを登録する

1. の管理アカウントの認証情報 AWS Management Console を使用して にサインインします AWS Organizations。RegisterDelegatedAdministrator API を実行するには、管理アカウントの認証情報が必要です。

2. IAM Identity Center が有効になっているリージョンを選択し、「IAM Identity Center コンソール」を開きます。
3. [設定] を選択し、[管理] タブを選択します。
4. [の委任管理者]セクションで、[登録] を選択します。
5. 委任された管理者の登録ページで、登録する AWS アカウント を選択し、アカウントの登録 を選択します。

メンバーアカウントを登録解除する

メンバーアカウントは、管理アカウントの認証情報を使用してサインインした場合にのみ、登録解除できます。

委任された管理者として以前に指定された AWS 組織のメンバーアカウントを登録解除して、IAM Identity Center から管理アクセスを削除するには、次の手順に従います。

> **Important**
>
> アカウントの登録を解除すると、すべての管理者ユーザーがそのアカウントから IAM Identity Center を管理できなくなります。その結果、このアカウントから IAM Identity Center ID、アクセス管理、認証、またはアプリケーションアクセスを管理できなくなります。このオペレーションは、IAM Identity Center で設定されたアクセス許可や割り当てには影響しないため、エンドユーザーは引き続きアプリケーションや AWS アクセスポータル内 AWS アカウント からアクセスできるため、エンドユーザーには影響しません。

メンバーアカウントを登録解除する

1. の管理アカウントの認証情報 AWS Management Console を使用して にサインインします AWS Organizations。DeregisterDelegatedAdministrator API を実行するには、管理アカウントの認証情報が必要です。
2. IAM Identity Center が有効になっているリージョンを選択し、「IAM Identity Center コンソール」を開きます。
3. [設定] を選択し、[管理] タブを選択します。
4. [委任管理者]セクションで、[登録解除] を選択します。
5. [アカウントの登録解除] ダイアログボックスでセキュリティ上の影響を確認し、メンバーアカウントの名前を入力して内容がわかっていることを確認します。

6. [アカウントの登録解除] を選択します。

委任管理者として登録されているメンバーアカウントが表示されます。

IAM Identity Center の委任管理者として設定 AWS Organizations されている のメンバーアカウントを確認するには、次の手順を使用します。

登録済みのメンバーアカウントを表示するには

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. [詳細] セクションで、[委任管理者] の下にある登録済みアカウント名を探します。この情報は、[管理] タブを選択し、[委任管理者] セクションで表示することでも確認できます。

一時的な昇格アクセス

へのすべてのアクセス AWS アカウント には、ある程度の権限が必要です。本番環境など、価値の高いリソースの設定を変更するなどの機密性の高いオペレーションには、範囲と潜在的な影響のために特別な処理が必要です。一時的な昇格アクセス (just-in-time アクセスとも呼ばれます) は、指定された時間内に特定のタスクを実行するアクセス許可の使用をリクエスト、承認、追跡する方法です。一時的な昇格アクセスは、権限セットや多要素認証など、他の形式のアクセス制御を補完します。

AWS IAM Identity Center では、さまざまなビジネス環境や技術環境での一時的な昇格されたアクセス管理に、次のオプションが用意されています。

- ベンダー管理のソリューションとサポートされているソリューション – AWS は、厳選されたパートナーサービスの IAM Identity Center 統合を検証し、共通の顧客要件 のセットに照らしてそれらの機能を評価しました。シナリオに最も合ったソリューションを選択し、プロバイダーのガイダンスに従って IAM Identity Center の機能を有効にしてください。
- セルフマネージド型およびセルフサポート型 – このオプションは、 AWS のみへの一時的な昇格アクセスに関心があり、 機能を自分でデプロイ、調整、維持できる場合の出発点となります。詳細については、「一時的な昇格アクセス管理 (TEAM)」を参照してください。

一時的な昇格アクセスについて検証済みの AWS セキュリティパートナー

AWS セキュリティパートナーは、さまざまなアプローチを使用して、一時的な昇格されたアクセス要件の一般的なセットに対処します。ビジネス、クラウド環境のアーキテクチャ、予算など、ニーズ

や好みに最適なソリューションを選択できるように、各パートナーソリューションを慎重に確認することをお勧めします。

> **Note**
>
> ディザスタリカバリでは、中断が発生する前に への緊急アクセスを設定する AWS Management Consoleことをお勧めします。

AWS Identity は、 AWS セキュリティパートナーによる以下の just-in-time サービスについて、機能と IAM Identity Center との統合を検証しました。

- CyberArk Secure Cloud Access – の一部であるこのサービスはCyberArk Identity Security Platform、 AWS およびマルチクラウド環境へのオンデマンドの昇格アクセスをプロビジョニングします。承認は、ITSM または ChatOps ツールとの統合を通じて対処されます。すべてのセッションを記録して、監査とコンプライアンスを確保できます。
- Tenable (previously Ermetic) – Tenableプラットフォームには、 AWS およびマルチクラウド環境での管理オペレーションのための特権アクセスの just-in-timeプロビジョニングが含まれます。AWS CloudTrail アクセスログを含むすべてのクラウド環境のセッションログを単一のインターフェースで分析と監査に使用できます。この機能は、Slack や Microsoft Teams などのエンタープライズおよびデベロッパーツールと統合されます。
- Okta アクセスリクエスト – Okta Identity Governance の一部で、IAM Identity Center 外部 ID プロバイダー (IdP) と IAM Identity Center アクセス許可セットとして を使用して just-in-time アクセスリクエストワークフローを設定できますOkta。

このリストは、 が追加のパートナーソリューションの機能 AWS を検証し、これらのソリューションを IAM Identity Center と統合するために更新されます。

> **Note**
>
> リソースベースのポリシー、Amazon Elastic Kubernetes Service (Amazon EKS)、または AWS Key Management Service (AWS KMS) を使用している場合は、 just-in-time ソリューションを選択するリソースポリシー、Amazon EKS、および のアクセス許可セットの参照 AWS KMS前に「」を参照してください。

AWS パートナー検証のために評価される一時的な昇格されたアクセス機能

AWS ID は、、CyberArk Secure Cloud Access、および アクセスリクエストによって提供される一時的な昇格されたアクセス機能がTenable、以下の一般的な顧客要件に対応していることを検証しました。 Okta

- ユーザーは、 AWS アカウント、アクセス許可セット、期間、理由を指定して、ユーザーが指定した期間、アクセス許可セットへのアクセスをリクエストできます。
- ユーザーはリクエストの承認ステータスを受け取ることができます。
- 同じスコープの承認済みリクエストがあり、承認済み期間中にセッションを呼び出す場合を除き、ユーザーは特定のスコープでセッションを呼び出すことはできません。
- リクエストを承認できるユーザーを指定する方法があります。
- 承認者は自分のリクエストを承認できません。
- 承認者には、保留中、承認済み、拒否済みのリクエストのリストがあり、監査人向けにエクスポートできます。
- 承認者は保留中のリクエストを承認および拒否できます。
- 承認者は、決定を説明するメモを追加できます。
- 承認者は承認されたリクエストを取り消すことができるため、昇格されたアクセスを今後使用できなくなります。

> **Note**
>
> 承認されたリクエストが取り消されたときに、昇格されたアクセスでユーザーがサインインした場合、そのセッションは、承認が取り消されてから最大 1 時間はアクティブのままになります。認証セッションの情報については、「認証」を参照してください。

- ユーザーアクションと承認は監査可能です。

へのシングルサインオンアクセス AWS アカウント

接続されたディレクトリ内のユーザーには、一般的な職務機能 AWS Organizations に基づいて、 の管理アカウントまたは組織内のメンバーアカウントに許可を割り当てることができます。または、特定のセキュリティ要件を満たすようにカスタムのアクセス権限を使用することもできます。例えば、データベース管理者には、開発用アカウントでは Amazon RDS に対する広範なアクセス権限を

付与しますが、本番稼働用アカウントではそれらのアクセス権限を制限します。IAM Identity Center によって、 AWS アカウント で必要なすべてのユーザーアクセス権限が自動的に設定されます。

> **Note**
>
> AWS Organizations 管理アカウントで運用するためのアクセス許可をユーザーまたはグループに付与する必要がある場合があります。権限の高いアカウントであるため、追加のセキュリティ制限により、これを設定する前に IAMFullAccess ポリシーまたは同等のアクセス許可が必要です。これらの追加のセキュリティ制限は、 AWS 組織内のメンバーアカウントでは必要ありません。

へのユーザーアクセスを割り当てる AWS アカウント

接続先ディレクトリのユーザーとグループにシングルサインオン· アクセスを割り当て、アクセス権限セットによってそれらのユーザーとグループのアクセスレベルを決定するには、以下の手順を実行します。

既存のユーザーおよびグループのアクセスを確認するには、「」を参照してくださいユーザーとグループの割り当てを表示する。

> **Note**
>
> アクセス権限の管理をシンプルにするために、個々のユーザーではなくグループに直接アクセスを割り当てることをお勧めします。グループを使用すると、個々のユーザーにこれらのアクセス権限を適用するのではなく、ユーザーグループに対してアクセス権限を付与または拒否できます。ユーザーが別の組織に異動した場合、そのユーザーを別のグループに移動するだけで、新しい組織に必要なアクセス権限がそのユーザーに自動的に付与されます。

ユーザーまたはグループアクセスを に割り当てるには AWS アカウント

1. IAM Identity Center コンソール を開きます。

   > **Note**
   >
   > 次のステップに進む前に、IAM Identity Center コンソールで、 AWS Managed Microsoft AD ディレクトリが存在するリージョンを使用していることを確認してください。

2. ナビゲーションペインの [マルチアカウントのアクセス許可] で、[AWS アカウント] を選択します。
3. [AWS アカウント] ページには、組織のツリービューリストが表示されます。シングルサインオンアクセスを割り当てる 1 つまたは複数の AWS アカウント の横にあるチェックボックスをオンにします。

> **Note**
>
> ユーザーとグループにシングルサインオンアクセスを割り当てる場合 AWS アカウント 、アクセス許可セットごとに一度に最大 10 を選択できます。10 個を超えるユーザーとグループ AWS アカウント を同じセットに割り当てるには、追加のアカウントで必要に応じてこの手順を繰り返します。プロンプトが表示されたら、同じユーザー、グループ、権限セットを選択します。

4. [ユーザーまたはグループの割り当て] を選択します。
5. ステップ 1: ユーザーとグループの選択では、ユーザーとグループを「*AWS-account-name*」に割り当てるページで、次の操作を行います。

   1. [ユーザー] タブで、シングルサインオン· アクセスを許可するユーザーを 1 人以上選択します。

      結果をフィルタリングするには、検索ボックスに目的のユーザーの名前を入力します。

   2. [グループ] タブで、シングルサインオン· アクセスを許可するグループを 1 つ以上選択します。

      結果をフィルターする場合は、検索ボックスに目的のグループの名前を入力します。

   3. 選択したユーザーとグループを表示するには、[選択したユーザーとグループ] の横にある横向きの三角形を選択します。
   4. 正しいユーザーとグループが選択されたことを確認したら、[次へ] を選択します。

6. ステップ 2: 権限セットの選択では、権限セットを「*AWS-account-name*」に割り当てるページで、次の操作を行います。

   1. 1 つまたは複数の権限セットを選択します。必要に応じて、新しい権限セットを作成して選択できます。

      - 1 つ以上の既存の権限セットを選択するには、[権限セット] で、前のステップで選択したユーザーとグループに適用する権限セットを選択します。

- 1 つ以上の新しい権限セットを作成するには、[権限セットの作成] を選択し、アクセス権限セットを作成します。 の手順に従います。適用する権限セットを作成したら、IAM Identity Center コンソールで「AWS アカウント」に戻り、「ステップ 2: 権限セットを選択する」が表示されるまで指示に従います。このステップに到達したら、作成した新しい権限セットを選択し、この手順の次のステップに進みます。

2. 正しい権限セットが選択されていることを確認したら、[次へ] を選択します。

7. ステップ 3: 確認して送信では、「***AWS-account-name***」への課題のレビューと提出ページで、次の操作を行います。

   1. 選択したユーザ、グループ、権限セットを確認します。
   2. 正しいユーザ、グループ、権限セットが選択されていることを確認したら、[提出] を選択します。

> **Important**
>
> ユーザーとグループへの割り当てプロセスが完了するまでに数分かかることがあります。プロセスが正常に完了するまで、このページを開いたままにしておきます。

> **Note**
>
> AWS Organizations 管理アカウントで運用するためのアクセス許可をユーザーまたはグループに付与する必要がある場合があります。権限の高いアカウントであるため、追加のセキュリティ制限により、これを設定する前に IAMFullAccess ポリシーまたは同等のアクセス許可が必要です。これらの追加のセキュリティ制限は、 AWS 組織内のメンバーアカウントでは必要ありません。

ユーザーとグループのアクセス権限を削除

この手順を使用して、接続されたディレクトリ内の AWS アカウント 1 つ以上のユーザーとグループの へのシングルサインオンアクセスを削除します。

へのユーザーおよびグループのアクセスを削除するには AWS アカウント

1. IAM Identity Center コンソール を開きます。

2. ナビゲーションペインの [マルチアカウントのアクセス許可] で、[AWS アカウント] を選択します。
3. [AWS アカウント] ページには、組織のツリービューリストが表示されます。シングルサインオンアクセスを削除するユーザーとグループ AWS アカウント を含む の名前を選択します。
4. の概要ページの「割り当てられたユーザーとグループ AWS アカウント」で、1 つ以上のユーザーまたはグループの名前を選択し、「アクセスの削除」を選択します。
5. [アクセス許可の削除] ダイアログで、ユーザーまたはグループの名前が正しいことを確認し、[アクセス許可の削除] を選択します。

アクセス許可セットによって作成されたアクティブな IAM ロールセッションを取り消す

以下は、IAM Identity Center ユーザーのアクティブなアクセス許可セットセッションを取り消すための一般的な手順です。この手順では、認証情報を侵害されたユーザーまたはシステム内の悪意のあるアクターに対するすべてのアクセスを削除することを前提としています。前提条件は、「」のガイダンスに従うことですアクセス許可セットによって作成されたアクティブな IAM ロールセッションを取り消すための準備。すべてのポリシーの拒否がサービスコントロールポリシー (SCP) に存在することを前提としています。

> **Note**
>
> AWS では、コンソールのみのオペレーションを除くすべてのステップを処理するオートメーションを構築することをお勧めします。

1. アクセスを取り消す必要があるユーザーのユーザー ID を取得します。ID ストア APIsを使用して、ユーザー名でユーザーを検索できます。
2. 拒否ポリシーを更新して、サービスコントロールポリシー (SCP) のステップ 1 のユーザー ID を追加します。このステップを完了すると、ターゲットユーザーはアクセスを失い、ポリシーが影響するロールでアクションを実行できなくなります。
3. ユーザーのアクセス許可セットの割り当てをすべて削除します。グループメンバーシップを通じてアクセスが割り当てられている場合は、すべてのグループとすべての直接アクセス許可セットの割り当てからユーザーを削除します。このステップにより、ユーザーは追加の IAM ロールを引き受けることができません。ユーザーがアクティブな AWS アクセスポータルセッションを持っていて、ユーザーを無効にすると、アクセスを削除するまで新しいロールを引き受け続けることができます。

4. ID プロバイダー (IdP) または Microsoft Active Directory を ID ソースとして使用する場合は、ID ソースのユーザーを無効にします。 ユーザーを無効にすると、追加の AWS アクセスポータルセッションが作成されなくなります。IdP または Microsoft Active Directory API ドキュメントを使用して、このステップを自動化する方法について説明します。IAM Identity Center ディレクトリを ID ソースとして使用している場合は、まだユーザーアクセスを無効にしないでください。ステップ 6 では、ユーザーアクセスを無効にします。
5. IAM Identity Center コンソールでユーザーを検索し、アクティブなセッションを削除します。

   a. [ユーザー] を選択します。
   b. アクティブなセッションを削除するユーザーを選択します。
   c. ユーザーの詳細ページで、アクティブセッションタブを選択します。
   d. 削除するセッションの横にあるチェックボックスをオンにし、セッションの削除 を選択します。

   これにより、ユーザーの AWS アクセスポータルセッションは約 60 分以内に停止します。セッション期間 について説明します。
6. IAM Identity Center コンソールで、ユーザーアクセスを無効にします。

   a. [ユーザー] を選択します。
   b. アクセスを無効にするユーザーを選択します。
   c. ユーザーの詳細ページで、一般情報を展開し、ユーザーアクセスの無効化ボタンを選択して、ユーザーのログインがこれ以上発生しないようにします。
7. 拒否ポリシーは、少なくとも 12 時間そのままにします。それ以外の場合、アクティブな IAM ロールセッションを持つユーザーは、IAM ロールでアクションを復元します。12 時間待機すると、アクティブなセッションは期限切れになり、ユーザーは IAM ロールに再度アクセスできなくなります。

> **Important**
>
> ユーザーセッションを停止する前にユーザーのアクセスを無効にした場合 (ステップ 5 を完了せずにステップ 6 を完了した場合)、IAM Identity Center コンソールからユーザーセッションを停止できなくなります。ユーザーセッションを停止する前にユーザーアクセスを誤って無効にした場合は、ユーザーを再度有効にしてセッションを停止し、再度アクセスを無効にできます。

パスワードが侵害された場合にユーザーの認証情報を変更し、割り当てを復元できるようになりました。

マスターアカウントでユーザーとグループにシングルサインオン・アクセスを割り当てる権限を委任する

IAM Identity Center コンソールを使用して、管理アカウントへのシングルサインオン・アクセスを割り当てるのは特権的アクションです。デフォルトでは、 AWS アカウントのルートユーザー または AWSSSOMasterAccountAdministratorと IAMFullAccess AWS 管理ポリシーがアタッチされているユーザーのみが、管理アカウントにシングルサインオンアクセスを割り当てることができます。AWSSSOMasterAccountAdministrator および IAMFullAccessポリシーは、 AWS Organizations 組織内の管理アカウントへのシングルサインオンアクセスを管理します。

ディレクトリ内のユーザーへのシングルサインオン・アクセスを管理するためにアクセス権限を委任するには、次の手順を実行します。

ディレクトリ内のユーザーへのシングルサインオン・アクセスを管理するためのアクセス権限を付与するには

1. 管理アカウントのルートユーザーまたは管理アカウントに IAM 管理者権限を持つ別の IAM ユーザーとして IAM Identity Center コンソールにサインインします。
2. アクセス権限セットを作成します。 の手順に従って権限セットを作成し、次の操作を行います。

    1. [新しい権限セットの作成] ページで [カスタム権限セットの作成] チェックボックスをオンにし、[次へ:詳細] を選択します。
    2. [新しい権限セットの作成] ページで、カスタム権限セットの名前と、必要に応じて説明を指定します。必要に応じて、セッション期間を変更し、リレーステート URL を指定します。

        > **Note**
        >
        > リレーステート URL には、 AWS Management Consoleに含まれている URL を指定する必要があります。例:
        >
        > **`https://console.aws.amazon.com/ec2/`**
        >
        > 詳細については、「リレーステートの設定」を参照してください。

    3. [どのポリシーを権限セットに含めたいですか?] で、[AWS 管理ポリシーを添付する] チェックボックスを選択します。

4. IAM ポリシーのリストで、 AWSSSOMasterAccountAdministratorと IAMFullAccess AWS の両方の管理ポリシーを選択します。これらのポリシーは、将来的にこのアクセス権限セットへのアクセスが割り当てられるすべてのユーザーとグループにアクセス権限を付与します。
5. [Next: Tags] (次へ: タグ) を選択します。
6. [Add tags (optional)] (タグの追加 (オプション)) で [Key] (キー) と [Value (optional)] (値 (オプション)) の値を指定して、[Next: Review] (次へ: レビュー) を選択します。タグの詳細については、AWS IAM Identity Center リソースのタグ付けを参照してください。
7. 選択した値を確認したら、[Create] (作成) を選択します。

3. へのユーザーアクセスを割り当てる AWS アカウント の手順に従って、作成した権限セットに適切なユーザーとグループを割り当てます。
4. 割り当てられたユーザーに以下を伝える: AWS アクセスポータルにサインインし、Accounts タブを選択すると、委任したアクセス許可で認証される適切なロール名を選択する必要があります。

アクセス権限セット

アクセス権限セットは、1 つまたは複数の [IAM policies] (IAM ポリシー) のコレクションの定義を作成および維持するテンプレートです。アクセス許可セットは、組織内のユーザーとグループの AWS アカウント アクセスの割り当てを簡素化します。例えば、 AWS RDS、DynamoDB、および Aurora サービスを管理するためのポリシーを含むデータベース管理者権限セットを作成し、その単一の権限セットを使用して、データベース管理者に AWS Organization AWS アカウント 内のターゲットのリストへのアクセスを許可できます。

IAM Identity Center は、アクセス許可セット AWS アカウント を使用して 1 つ以上の のユーザーまたはグループにアクセスを割り当てます。アクセス権限セットを割り当てると、IAM Identity Center は、対応する IAM Identity Center 制御の IAM ロールを各アカウントに作成し、アクセス権限セットで指定されたポリシーをそれらのロールに適用します。IAM Identity Center は、IAM Identity Center ユーザーポータルまたは AWS CLI を使用してロールを管理し、定義した認可されたユーザーがロールを引き受けることを許可します。 アクセス権限セットを変更すると、IAM Identity Center は、対応する IAM ポリシーとロールがそれに応じて更新されることを保証します。

アクセス権限セットには、AWS マネージドポリシー、カスタマー管理ポリシー、インラインポリシー、およびAWS 職務機能の管理ポリシーを追加できます。アクセス許可の境界として、 AWS マネージドポリシーまたはカスタマー管理ポリシーを割り当てることもできます。

アクセス権限セットを作成するには、「アクセス許可セットの作成、管理と削除」を参照してください。

トピック

事前定義済み権限

AWS 管理ポリシーを使用して事前定義されたアクセス許可セットを作成できます。

事前定義されたアクセス許可を持つアクセス許可セットを作成するときは、 AWS 管理ポリシーのリストから 1 つのポリシーを選択します。使用可能なポリシーの中で、共通権限ポリシー と職務機能ポリシー から選択できます。

共通のアクセス許可ポリシー

全体のリソースにアクセスできるようにする AWS マネージドポリシーのリストから選択します AWS アカウント。以下のいずれかのポリシーを追加できます。

- AdministratorAccess
- PowerUserAccess
- ReadOnlyAccess
- ViewOnlyAccess

職務機能ポリシー

組織内のジョブに関連する AWS アカウント 可能性のある 内のリソースへのアクセスを可能にする AWS マネージドポリシーのリストから選択します。以下のいずれかのポリシーを追加できます。

- Billing
- DataScientist
- DatabaseAdministrator
- NetworkAdministrator
- SecurityAudit

- SupportUser
- SystemAdministrator

使用可能な共通権限ポリシーとジョブ機能ポリシーの詳細については、AWS Identity and Access Management ユーザーガイドの AWS 職務機能の管理ポリシー を参照してください。

アクセス権限セットの作成方法については、「アクセス許可セットの作成、管理と削除」を参照してください。

カスタムアクセス許可

カスタムアクセス許可 を使用してアクセス許可セットを作成し、 AWS Identity and Access Management (IAM) で保持している AWS 管理ポリシーとカスタマー管理ポリシーをインラインポリシーと組み合わせることができます。また、アクセス許可の境界を含めて、他のポリシーがアクセス許可セットのユーザーに付与できるアクセス許可の上限を設定することもできます。

アクセス権限セットの作成方法については、「アクセス許可セットの作成、管理と削除」を参照してください。

アクセス権限セットに適用できるポリシータイプ

トピック

- インラインポリシー
- AWS マネージドポリシー
- カスタマー管理ポリシー
- アクセス許可の境界

インラインポリシー

インラインポリシーをアクセス権限セットに適用します。インラインポリシーは IAM ポリシーとしてフォーマットされたテキストブロックで、アクセス権限セットに直接追加します。新しいアクセス権限セットを作成するときに、ポリシーを貼り付けるか、IAM Identity Center コンソールのポリシー作成ツールを使用して新しいポリシーを生成できます。AWS ポリシージェネレーター を使用して IAM ポリシーを作成することもできます。

インラインポリシーを使用してアクセス許可セットをデプロイすると、IAM Identity Center はアクセス許可セット AWS アカウント を割り当てる に IAM ポリシーを作成します。IAM Identity Center

は、アクセス権限セットをアカウントに割り当てるとポリシーを作成します。その後、ポリシーは、ユーザーが引き受け AWS アカウント る の IAM ロールにアタッチされます。

インラインポリシーを作成してアクセス許可セットを割り当てると、IAM Identity Center によってのポリシーが自動的に設定されます AWS アカウント 。を使用してアクセス許可セットを構築する場合はカスタマー管理ポリシー、アクセス許可セットを割り当てる前に、 AWS アカウント でポリシーを作成する必要があります。

AWS マネージドポリシー

AWS 管理ポリシーをアクセス許可セットにアタッチできます。 AWS 管理ポリシーは、 が AWS 維持する IAM ポリシーです。これとは対照的に、 カスタマー管理ポリシーは、作成して管理するアカウントの IAM ポリシーです。 AWS 管理ポリシーは、 の一般的な最小特権のユースケースに対処します AWS アカウント。 AWS 管理ポリシーは、IAM Identity Center が作成するロールのアクセス許可として、またはアクセス許可の境界として割り当てることができます。

AWS はAWS 、 リソースにジョブ固有のアクセス許可を割り当てるジョブ機能の マネージドポリシーを維持します。 AWS アクセス権限セットに 定義済みの権限 を使用する場合は、職務ポリシーを 1 つ追加できます。カスタム権限 を選択すると、複数の職務ポリシーを追加できます。

AWS アカウント また、 には、 の特定の AWS のサービス および の組み合わせに対する多数の AWS マネージド IAM ポリシーが含まれています AWS のサービス。カスタムアクセス許可 を使用してアクセス許可セットを作成する場合、アクセス許可セットに割り当てる多くの追加の AWS 管理ポリシーから選択できます。

AWS は、すべての AWS アカウント に AWS マネージドポリシーを設定します。 AWS 管理ポリシーを使用してアクセス許可セットをデプロイするには、まず でポリシーを作成する必要はありません AWS アカウント。を使用してアクセス許可セットを構築する場合はカスタマー管理ポリシー、アクセス許可セットを割り当てる前に、 AWS アカウント でポリシーを作成する必要があります。

AWS 管理ポリシーの詳細については、「IAM ユーザーガイド」の「 AWS 管理ポリシー」を参照してください。

カスタマー管理ポリシー

カスタマー管理ポリシーをアクセス権限セットに適用できます。カスタマー管理ポリシーは、アカウント内で顧客が作成および維持する IAM ポリシーです。対照的に、 AWS マネージドポリシーは が AWS 維持するアカウントの IAM ポリシーです。カスタマー管理ポリシーは、IAM Identity Center が作成するロールのアクセス権限として、または アクセス許可の境界 として割り当てることができます。

カスタマー管理ポリシーを使用してアクセス許可セットを作成する場合、IAM Identity Center AWS アカウント がアクセス許可セットを割り当てる各 で、同じ名前とパスの IAM ポリシーを作成する必要があります。カスタムパスを指定する場合は、必ず各 AWS アカウントに同じパスを指定してください。詳細については、「IAM ユーザーガイド」の「親しみやすい名前とパス」を参照してください。IAM Identity Center は、作成した IAM ポリシーを、 AWS アカウントで作成した IAM ロールにアタッチします。ベストプラクティスとして、アクセス権限セットを割り当てる各アカウントのポリシーに同じアクセス権限を適用します。詳細については、「権限セットに IAM ポリシーを使用する」を参照してください。

詳細については、IAM ユーザーガイドの「カスタマー管理ポリシー」を参照してください。

アクセス許可の境界

アクセス権限セットには アクセス許可の境界を適用できます。アクセス許可の境界は、アイデンティティベースのポリシーが IAM プリンシパルに付与できるアクセス許可の上限を設定する AWS マネージドまたはカスタマーマネージド IAM ポリシーです。アクセス許可の境界を適用する場合、インラインポリシー、カスタマー管理ポリシー、および AWS マネージドポリシーは、そのアクセス許可の境界によって付与されるアクセス権限を超えるアクセス権限を付与することはできません。アクセス許可の境界ではアクセス権限は付与されませんが、その代わりに IAM が境界を超えるすべてのアクセス権限を無視するようになります。

カスタマー管理ポリシーをアアクセス許可の境界として使用して権限セットを作成する場合、IAM Identity Center が権限セットを割り当てる各 AWS アカウント に同じ名前の IAM ポリシーを作成する必要があります。IAM Identity Center は、IAM ポリシーをアクセス許可の境界として AWS アカウント で作成する IAM ロールに適用します。

詳細については、IAM ユーザーガイド の IAM エンティティのアクセス許可の境界を参照してください。

アクセス許可セットの作成、管理と削除

アクセス権限セットは、ユーザーおよびグループが持つこの AWS アカウントアカウントに対するアクセスのレベルを定義します。権限セットは IAM Identity Center に保存され、1 つまたは複数の AWS アカウントにプロビジョニングできます。複数のアクセス権限セットを 1 人のユーザーに割り当てることができます。IAM Identity Center でのアクセス許可セットの使用方法の詳細については、アクセス権限セット を参照してください。

アクセス許可セットを作成するときは、次の考慮事項に留意してください。

- あらかじめ定義されたアクセス許可セットから始める

事前定義されたアクセス許可セットでは、事前定義されたアクセス許可 を使用して、使用可能なポリシーのリストから 1 つの AWS 管理ポリシーを選択します。各ポリシーは、 AWS サービスおよびリソースへの特定のレベルのアクセス、または共通の職務機能に対するアクセス許可を付与します。これらのポリシーそれぞれの詳細については、「AWS 職務機能の管理ポリシー」を参照してください。使用状況データを収集したら、アクセス許可セットをより制限の厳しいものに調整できます。

- 管理セッションの期間を妥当な作業期間に制限する

  ユーザーが にフェデレーション AWS アカウント し、 AWS マネジメントコンソールまたは AWS コマンドラインインターフェイス (AWS CLI) を使用する場合、IAM Identity Center はアクセス許可セットのセッション期間設定を使用してセッション期間を制御します。ユーザーセッションがセッション時間に達すると、コンソールからサインアウトされ、再度サインインするよう求められます。セキュリティのベストプラクティスとして、ロールを実行するために必要な長さを超えるセッション期間を設定しないことをお勧めします。デフォルトでは、[セッション期間] は 1 時間です。最大値は 12 時間まで指定できます。詳細については、「セッション期間の設定」を参照してください。

- ワークフォースユーザーポータルのセッション期間を制限する

  ワークフォースユーザーはポータルセッションを使用してロールを選択し、アプリケーションにアクセスします。デフォルトでは、最大セッション期間 の値は、ワークフォースユーザーが再認証される前に AWS アクセスポータルにサインインできる時間の長さを決定し、8 時間です。最大値は 90 日まで指定できます。詳細については、「AWS アクセスポータルと IAM Identity Center 統合アプリケーションのセッション期間を設定する」を参照してください。

- 最小特権アクセス許可を与えるロールを使用する

  作成してユーザーに割り当てる各アクセス許可セットは、 AWS アクセスポータルで使用可能なロールとして表示されます。そのユーザーとしてポータルにサインインするときは、アカウント内のタスクの実行に使用できる最も制限の厳しいアクセス権限セットに対応するロールを (`AdministratorAccess` ではなく) 選択してください。ユーザー招待を送信する前に、アクセス許可セットをテストして必要なアクセス許可が提供されていることを確認してください。

> **Note**
>
> AWS CloudFormation を使用してアクセス許可セットを作成して割り当て、それらのアクセス許可セットにユーザーを割り当てることもできます。

トピック

アクセス権限セットを作成します。

この手順を使用して、1 つの AWS 管理ポリシーを使用する定義済みの権限セット、または最大 10 個の AWS 管理ポリシーまたはカスタマー管理ポリシーとインラインポリシーを使用するカスタム権限セットを作成します。IAM の「Service Quotas コンソール」で、ポリシーの最大数 10 への調整をリクエストできます。

IAM Identity Center コンソールで権限セットを作成できます。

アクセス権限セットを作成するには

1. IAM Identity Center コンソール を開きます。
2. [マルチアカウント権限] で、[権限セット] を選択します。
3. [Create permission set] (アクセス権限セットの作成) を選択します。
4. [権限セットタイプの選択] ページの [権限セットタイプ] で、権限セットタイプを選択します。
5. 権限セットタイプに基づいて、権限セットに使用したいポリシーを 1 つ以上選択します。

    - 定義済み権限セット
        1. 事前定義されたアクセス許可セットのポリシー で、リスト内の IAM ジョブ関数ポリシーまたは共通アクセス許可ポリシーのいずれかを選択し、次へ を選択します。詳細については、「AWS Identity and Access Management ユーザーガイド」の「AWS ジョブ機能の管理ポリシー」および「AWS マネージドポリシー」を参照してください。
        2. ステップ 6 に進み、権限セットの詳細の指定ページを完了します。
    - カスタム権限セット
        1. [次へ] をクリックします。
        2. ポリシーとアクセス許可の境界を指定ページで、新しいアクセス許可セットに適用する IAM ポリシーのタイプを選択します。デフォルトでは、最大 10 個の [AWS 管理ポリシー] と [顧客管理ポリシー] を任意に組み合わせて権限セットに追加できます。このクォータは IAM によって設定されます。これを増やすには、権限セットを割り当てたい各 AWS アカ

ウント で、Service Quotas コンソールの「IAM ロールにアタッチされている IAM クォータ管理ポリシー」の追加をリクエストします。

- AWS 管理ポリシーを展開して、IAM からポリシーを追加して、 AWS 構築および維持します。詳細については、「AWS マネージドポリシー」を参照してください。

  a. [AWS 権限セット] でユーザーに適用する管理ポリシーを検索して選択します。

  b. 別の種類のポリシーを追加する場合は、そのコンテナを選択して選択します。適用するポリシーをすべて選択したら、[次へ] を選択します。ステップ 6 に進み、アクセス許可セットの詳細の指定ページを完了します。

- [顧客管理ポリシー] を展開して、作成して管理するポリシーを IAM から追加します。詳細については、「カスタマー管理ポリシー」を参照してください。

  a. [ポリシーを追加] を選択し、権限セットに追加するポリシーの名前を入力します。権限セットを割り当てる各アカウントで、入力した名前でポリシーを作成します。ベストプラクティスとして、各アカウントのポリシーに同じ権限を割り当ててください。

  b. [もっと追加する] を選択して別のポリシーを追加します。

  c. 別の種類のポリシーを追加する場合は、そのコンテナを選択して選択します。適用するポリシーをすべて選択したら、[次へ] を選択します。ステップ 6 に進み、権限セットの詳細の指定ページを完了します。

- インラインポリシーを展開して、カスタム JSON 形式のポリシーテキストを追加します。インラインポリシーは既存の IAM リソースに対応していません。インラインポリシーを作成するには、表示されたフォームにカスタムポリシー言語を入力します。IAM Identity Center は、メンバーアカウントに作成した IAM リソースにポリシーを追加します。詳細については、「インラインポリシー」を参照してください。

  a. インタラクティブエディタ内の目的のアクションとリソースをインラインポリシーに追加します。追加のステートメントは、新しいステートメントを追加 で追加できます。

  b. 別の種類のポリシーを追加する場合は、そのコンテナを選択して選択します。適用するポリシーをすべて選択したら、[次へ] を選択します。ステップ 6 に進み、アクセス許可セットの詳細の指定ページを完了します。

- アクセス許可の境界を展開して、 AWS 管理またはカスタマー管理の IAM ポリシーを、アクセス許可セット内の他のポリシーが割り当てることができる最大アクセス許可として追加します。詳細については、「アクセス許可の境界」を参照してください。

  a. [アクセス許可の境界を使用する] を選択して、アクセス許可の上限を設定します。

b. [AWS 管理ポリシー] を選択し、IAM からポリシーを設定し、「AWS」がアクセス許可の境界として構築・維持します。[カスタマー管理ポリシー] を選択して、[お客様] が IAM から作成して維持するポリシーをアクセス許可の境界として設定します。

c. 別の種類のポリシーを追加する場合は、そのコンテナを選択して選択します。適用するポリシーをすべて選択したら、[次へ] を選択します。ステップ 6 に進み、権限セットの詳細の指定ページを完了します。

6. [権限セットの詳細指定] ページで、以下を実行します。

1. [権限セット名] に、IAM Identity Center でこの権限セットを識別するための名前を入力します。このアクセス許可セットに指定した名前は、利用可能なロールとして AWS アクセスポータルに表示されます。ユーザーは AWS アクセスポータルにサインインし、 を選択し AWS アカウント、ロールを選択します。

2. (オプション) 説明を入力することもできます。説明は、 AWS アクセスポータルではなく、IAM Identity Center コンソールにのみ表示されます。

3. (オプション) Session duration (セッション期間) の値を指定します。この値は、コンソールがユーザーをセッションからログアウトさせるまでのログオン時間の長さを決定します。詳細については、「セッション期間の設定」を参照してください。

4. (オプション) Relay state (リレーステート) の値を指定します。この値は、フェデレーションプロセスにおいて、アカウント内のユーザーをリダイレクトするために使用されます。詳細については、「リレーステートの設定」を参照してください。

> **Note**
>
> リレーステート URL は AWS Management Console内にある必要があります。例: **`https://console.aws.amazon.com/ec2/`**

5. [タグ (オプション)] を拡張して [タグの追加] を選択し、[キー] と [値 (オプション)] () の値を指定します。

   タグの詳細については、「AWS IAM Identity Center リソースのタグ付け」を参照してください。

6. [次へ] をクリックします。

7. [確認と作成] ページで、選択した内容を確認し、[作成] を選択します。

8. デフォルトでは、アクセス許可セットを作成すると、アクセス許可セットはプロビジョニングされません (どの でも使用されます AWS アカウント) 。でアクセス許可セットをプロビジョニングするには AWS アカウント、アカウント内のユーザーとグループに IAM Identity Center アクセ

スを割り当ててから、アクセス許可セットをそれらのユーザーとグループに適用する必要があります。詳細については、「へのシングルサインオンアクセス AWS アカウント」を参照してください。

権限セット管理の委任

IAM Identity Center では、IAM Identity Center リソースの Amazon リソースネーム (ARN) を参照する IAM ポリシーを作成することで、アカウントのアクセス権限セットや割り当ての管理を委任することができます。例えば、特定のタグが付いたアクセス権限セットの特定のアカウントでの割り当てを、異なる管理者が管理できるようなポリシーを作成することができます。

このようなポリシーを作成するには、以下の方法があります。

- (推奨) IAM Identity Center で権限セットを作成し、それぞれに異なるポリシーを設定して、アクセス権限セットを異なるユーザーまたはグループに割り当てます。これにより、選択した IAM Identity Center アイデンティティソースを使用してサインインしたユーザーの管理権限を管理することができます。
- IAM でカスタムポリシーを作成し、管理者が想定する IAM ロールにアタッチします。ロールについては、割り当てられた IAM Identity Center 管理権限を取得するための「IAM ロール」を参照してください。

> **Important**
>
> IAM Identity Center リソースの ARN は、大文字と小文字を区別します。

以下は、IAM Identity Center 権限セットとアカウントリソースタイプを参照する適切なケースです。

リソースタイプ	ARN	コンテキストキー
PermissionSet	`arn:${Partition}:sso:::permissionSet/${InstanceId}/${PermissionSetId}`	`aws:ResourceTag/${TagKey}`

リソースタイプ	ARN	コンテキストキー
アカウント	`arn:${Partition}:sso:::account/${AccountId}`	該当しません

権限セットに IAM ポリシーを使用する

アクセス権限セットを作成します。 では、カスタマー管理ポリシーや権限境界などのポリシーを権限セットに追加する方法を学習しました。カスタマーが管理するポリシーと権限を権限セットに追加すると、IAM Identity Center はどの AWS アカウントでもポリシーを作成しません。その代わりに、権限セットを割り当てたい各アカウントで事前にそれらのポリシーを作成し、権限セットの名前とパスの指定に一致させる必要があります。組織 AWS アカウント 内の にアクセス許可セットを割り当てると、IAM Identity Center は AWS Identity and Access Management (IAM) ロールを作成し、そのロールに IAM ポリシーをアタッチします。

> **Note**
>
> IAM ポリシーを使用して権限セットを割り当てる前に、メンバーアカウントを準備する必要があります。メンバーアカウントの IAM ポリシーの名前は、管理アカウントのポリシー名と大文字と小文字が区別される必要があります。ポリシーがメンバーアカウントに存在しない場合、IAM Identity Center は権限セットを割り当てることができません。
> ポリシーによって付与される権限は、アカウント間で完全に一致する必要はありません。

IAM ポリシーをアクセス許可セットに割り当てるには

1. アクセス許可セット AWS アカウント を割り当てる各 に IAM ポリシーを作成します。
2. IAM ポリシーにアクセス許可を割り当てます。アカウントごとに異なるアクセス許可を割り当てることができます。一貫した操作性を実現するには、各ポリシーで同じ権限を設定し、維持してください。などのオートメーションリソースを使用して、各メンバーアカウントで同じ名前とアクセス許可を持つ IAM ポリシーのコピー AWS CloudFormation StackSets を作成できます。の詳細については CloudFormation StackSets、「 ユーザーガイド」の AWS CloudFormation StackSets「 の使用AWS CloudFormation 」を参照してください。
3. 管理アカウントに権限セットを作成し、[カスタマー管理ポリシー] または [アクセス許可の境界] に IAM ポリシーを追加します。権限セットの作成方法の詳細については、アクセス権限セットを作成します。 を参照してください。

4. 準備したインラインポリシー、 AWS 管理ポリシー、その他の IAM ポリシーを追加します。
5. 権限セットを作成して割り当てます。

アクセス権限セットを削除する

アクティブなアクセス許可セットセッションを取り消す場合は、「」を参照してくださいアクセス許可セットによって作成されたアクティブな IAM ロールセッションを取り消す。

IAM Identity Center から権限セットを削除する前に、権限セットを使用するすべての AWS アカウント から削除する必要があります。既存のユーザーおよびグループのアクセスを確認するには、「」を参照してくださいユーザーとグループの割り当てを表示する。

からアクセス許可セットを削除するには AWS アカウント

1. IAM Identity Center コンソール を開きます。
2. [マルチアカウント権限] で、[AWS アカウント] を選択します。
3. [AWS アカウント] ページには、組織のツリービューリストが表示されます。アクセス許可セットを削除する AWS アカウント の名前を選択します。
4. の概要ページで AWS アカウント、アクセス許可セットタブを選択します。
5. 削除する権限セットの横にあるチェックボックスをオンにし、[削除]を選択します。
6. [権限セットの削除] ダイアログボックスで、正しい権限セットが選択されていることを確認し、**Delete** と入力して削除を確認し、[アクセス権の削除] を選択します。

組織 AWS アカウント 内のどの でも使用できなくなるように、次の手順を使用して 1 つ以上のアクセス許可セットを削除します。

> **Note**
>
> このアクセス許可セットが割り当てられているすべてのユーザーとグループは、そのアクセス許可セット AWS アカウント を使用しているかどうかにかかわらず、サインインできなくなります。既存のユーザーおよびグループのアクセスを確認するには、「」を参照してくださいユーザーとグループの割り当てを表示する。

からアクセス許可セットを削除するには AWS アカウント

1. IAM Identity Center コンソール を開きます。

2. [マルチアカウント権限] で、[権限セット] を選択します。
3. 削除するアクセス権限セットを選択してから、[削除] を選択します。
4. [権限セットの削除] ダイアログボックスで、権限セットの名前を入力して削除を確認し、[削除] を選択します。名前は、大文字と小文字が区別されます。

アクセス権限セットのプロパティを構成する

IAM Identity Center では、以下のアプリケーションの権限セットのプロパティを設定することで、ユーザーエクスペリエンスをカスタマイズできます。

トピック

セッション期間の設定

権限セット毎に、ユーザーが AWS アカウントアカウントにサインインできる期間を制御するためのセッション期間を指定できます。指定された期間が経過すると、 はセッションからユーザー AWS に署名します。

新しいアクセス権限セットを作成すると、デフォルトでセッションの継続時間が 1 時間 (秒単位) に設定されます。セッション時間は、最短で 1 時間、最長で 12 時間まで設定できます。IAM Identity Center では、権限セットごとに割り当てられたアカウントに IAM ロールが自動的に作成され、これらのロールは最大セッション時間が 12 時間になるように構成されています。

ユーザーが AWS アカウント コンソールにフェデレーションする場合、または (AWS CLI) が使用されている場合 AWS Command Line Interface 、IAM Identity Center はアクセス許可セットのセッション期間設定を使用してセッション期間を制御します。デフォルトでは、IAM Identity Center によって生成された権限セットの IAM ロールは、IAM Identity Center ユーザーのみが引き受けることができます。これにより、IAM Identity Center 権限セットで指定されたセッション期間が適用されます。

> **Important**
>
> セキュリティのベストプラクティスとして、ロールを実行するために必要な長さを超えるセッション期間を設定しないことをお勧めします。

権限セットが作成された後、更新して、新しいセッションの有効期間を適用できます。特定の権限セットのセッション期間の長さを変更するには、次の手順を実行します。

セッション期間を設定するには

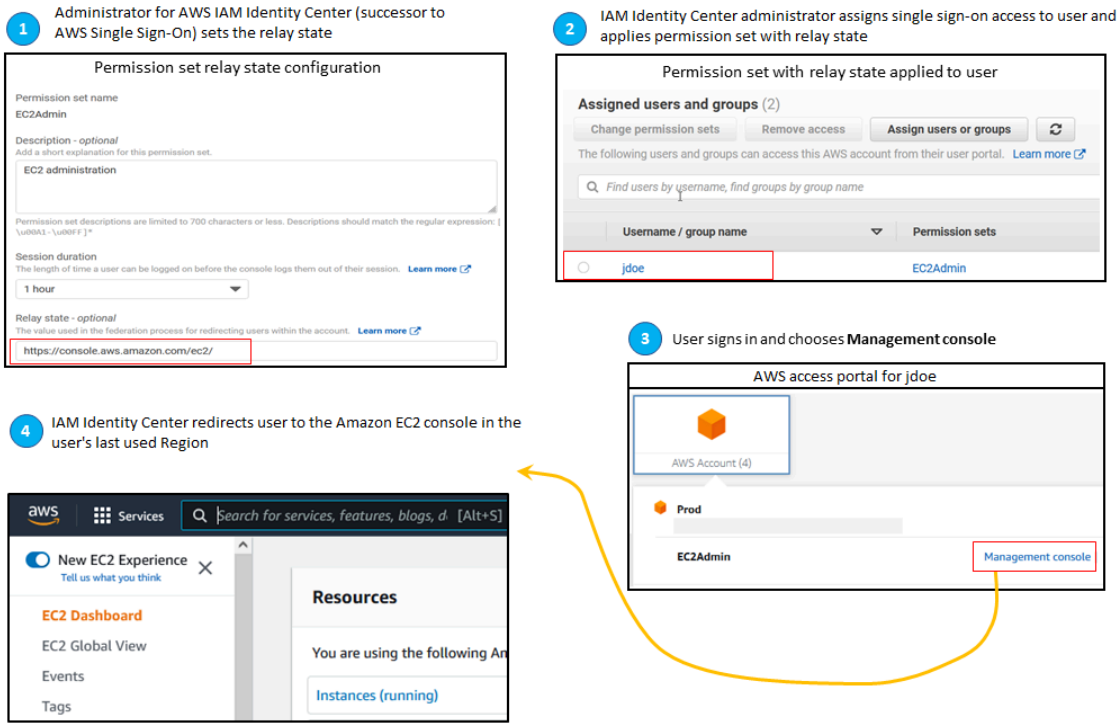
1. IAM Identity Center コンソール を開きます。
2. [マルチアカウント権限] で、[権限セット] を選択します。
3. セッション継続時間を変更する権限セットの名前を選択します。
4. 権限セットの詳細ページの [一般設定] セクションの見出しの右側で、[編集] を選択します。
5. [一般権限セット設定の編集] ページで、[セッション期間] に新しい値を選択します。
6. アクセス許可セットが でプロビジョニングされている場合 AWS アカウント、アカウントの名前は の下に表示されAWS アカウント 、自動的に を再プロビジョニングします。アクセス許可セットのセッション期間の値が更新されると、アクセス許可セット AWS アカウント を使用するすべての が再プロビジョニングされます。つまり、この設定の新しい値は、 アクセス許可セット AWS アカウント を使用するすべての に適用されます。
7. [変更を保存] を選択します。
8. [AWS アカウント] ページの上部に通知が表示されます。

   - 権限セットが 1 つまたは複数の AWS アカウントにプロビジョニングされている場合、通知は、 AWS アカウント が正常に再ビジョニングされ、更新された権限セットがアカウントに適用されたことを確認します。
   - アクセス許可セットが にプロビジョニングされていない場合 AWS アカウント、通知はアクセス許可セットの設定が更新されたことを確認します。

リレーステートの設定

デフォルトでは、ユーザーが AWS アクセスポータルにサインインし、アカウントを選択し、割り当てられたアクセス許可セットから が AWS 作成するロールを選択すると、IAM Identity Center はユーザーのブラウザを にリダイレクトします AWS Management Console。リレーステートを別のコンソール URL に設定することで、この動作を変更できます。リレーステートを設定すると、ユーザーは自分の役割に最も適したコンソールにすばやくアクセスできるようになります。たとえば、Amazon EC2 コンソール URL (**`https://console.aws.amazon.com/ec2/`**) にリレー状態を設定して、ユーザーが Amazon EC2 管理者ロールを選択したときにユーザーをそのコンソールにリダイレクトできます。デフォルトの URL またはリレーステート URL へのリダイレクト中、IAM Identity Center は、ユーザーが最後に AWS リージョン 使用した のコンソールエンドポイントにユーザーのブラウザをルーティングします。たとえば、ユーザーが欧州 (ストックホルム) リー

ジョン (eu-north-1) で最後のコンソールセッションを終了した場合、ユーザーはそのリージョンの Amazon EC2 コンソールにリダイレクトされます。



ユーザーを特定の AWS リージョンのコンソールにリダイレクトするように IAM Identity Center を設定するには、URL の一部にリージョン指定を含めます。たとえば、ユーザーを米国東部 (オハイオ) リージョン (us-east-2) の Amazon EC2 コンソールにリダイレクトするには、そのリージョン (**`https://us-east-2.console.aws.amazon.com/ec2/`**) の Amazon EC2 コンソールの URL を指定します。米国西部 (オレゴン) リージョン (us-west-2) リージョンで IAM Identity Center を有効にし、そのリージョンにユーザを誘導する場合は、**`https://us-west-2.console.aws.amazon.com`** を指定します。

特定の権限セットのリレーステート URL を変更するには、次の手順を実行します。

リレーステートを設定するには

1. IAM Identity Center コンソール を開きます。
2. [マルチアカウント権限] で、[権限セット] を選択します。
3. 新しいリレーステート URL を指定するアクセス権限セットの名前を選択します。
4. 権限セットの詳細ページの [一般設定] セクションの見出しの右側で、[編集] を選択します。

5. 「一般的なアクセス許可セット設定の編集」ページの「リレー状態」で、いずれかの AWS サービスのコンソール URL を入力します。例:

   `https://console.aws.amazon.com/ec2/`

   > **Note**
   >
   > リレーステート URL は AWS Management Console内にある必要があります。

6. アクセス許可セットが でプロビジョニングされている場合 AWS アカウント、アカウントの名前は の下に表示されAWS アカウント 、自動的に が再プロビジョニングされます。アクセス許可セットのリレーステート URL が更新されると、アクセス許可セット AWS アカウント を使用するすべての が再プロビジョニングされます。つまり、この設定の新しい値は、 アクセス許可セット AWS アカウント を使用するすべての に適用されます。
7. [変更を保存] を選択します。
8. [AWS 組織] ページの上部に通知が表示されます。

   - 権限セットが 1 つまたは複数の AWS アカウントにプロビジョニングされている場合、通知は、 AWS アカウント が正常に再ビジョニングされ、更新された権限セットがアカウントに適用されたことを確認します。
   - アクセス許可セットが にプロビジョニングされていない場合 AWS アカウント、通知はアクセス許可セットの設定が更新されたことを確認します。

> **Note**
>
> AWS API、 AWS SDK、または AWS Command Line Interface() を使用して、このプロセスを自動化できますAWS CLI。詳細については、以下を参照してください。
>
> - [IAM Identity Center API リファレンス] の `CreatePermissionSet` または `UpdatePermissionSet` アクション
> - [AWS CLI コマンドリファレンス] の [sso-admin] セクションにある `create-permission-set` または `update-permission-set` コマンド。

拒否ポリシーを使用してアクティブなユーザーのアクセス許可を取り消す

ユーザーがアクセス許可セットをアクティブに使用している AWS アカウント 間は、IAM Identity Center ユーザーの へのアクセスを取り消す必要がある場合があります。未指定ユーザーの拒否ポリシーを事前に実装することで、アクティブな IAM ロールセッションを使用する機能を削除できます。必要に応じて、拒否ポリシーを更新して、アクセスをブロックするユーザーを指定できます。このトピックでは、拒否ポリシーを作成する方法と、ポリシーをデプロイする方法に関する考慮事項について説明します。

アクセス許可セットによって作成されたアクティブな IAM ロールセッションを取り消すための準備

サービスコントロールポリシーを使用して、特定のユーザーのすべてのポリシーを拒否することで、ユーザーがアクティブに使用している IAM ロールでアクションを実行できないようにできます。また、パスワードを変更するまで、ユーザーがアクセス許可セットを使用することを禁止できます。これにより、盗まれた認証情報を悪用する悪意のある攻撃者が取り除かれます。アクセスを広く拒否し、ユーザーがアクセス許可セットを再入力したり、他のアクセス許可セットにアクセスしたりしないようにする必要がある場合は、すべてのユーザーアクセスを削除し、アクティブな AWS アクセスポータルセッションを停止し、ユーザーのサインインを無効にすることもできます。より広範なアクセス失効アクセス許可セットによって作成されたアクティブな IAM ロールセッションを取り消すのための追加のアクションと組み合わせて拒否ポリシーを使用する方法については、「」を参照してください。

ポリシーを拒否する

拒否ポリシーを IAM Identity Center ID ストアUserIDのユーザーの と一致する条件とともに使用して、ユーザーがアクティブに使用している IAM ロールによるそれ以上のアクションを防ぐことができます。このポリシーを使用すると、拒否ポリシーをデプロイするときに同じアクセス許可セットを使用している可能性のある他のユーザーへの影響を回避できます。このポリシーは、アクセスを取り消すユーザー ID で*Add user ID here*"identitystore:userId"更新する のプレースホルダーユーザー ID を使用します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "*"
            ],
            "Resource": "*",
```

```
            "Condition": {
                "StringEquals": {
                    "identitystore:userId": "Add user ID here"
                }
            }
        }
    ]
}
```

などの別の条件キーを使用できます“identitystore:userId”が“aws:userId”、これは 1 人のユーザーに関連付けられているグローバルに一意の値であるため、 は確実です。“aws:userId” 条件で を使用すると、ID のソースからユーザー属性が同期される方法に影響され、ユーザーのユーザー名または E メールアドレスが変更されると変更される可能性があります。

IAM Identity Center コンソールから、ユーザー に移動し、ユーザーを名前で検索し、一般情報セクションを展開し、ユーザー ID をコピーidentitystore:userIdすることで、ユーザーの を見つけることができます。また、ユーザー ID を検索しながら、ユーザーの AWS アクセスポータルセッションを停止し、同じセクションでサインインアクセスを無効にするのも便利です。ID ストア APIs をクエリしてユーザーのユーザー ID を取得することで、拒否ポリシーを作成するプロセスを自動化できます。

拒否ポリシーのデプロイ

など、無効なプレースホルダーユーザー ID を使用して*Add user ID here*、 AWS アカウントユーザーにアタッチしたサービスコントロールポリシー (SCP) を使用して、事前に拒否ポリシーをデプロイできます。これは、影響の容易さとスピードのために推奨されるアプローチです。拒否ポリシーを使用してユーザーのアクセスを取り消す場合、ポリシーを編集して、プレースホルダーユーザー ID を、アクセスを取り消すユーザーのユーザー ID に置き換えます。これにより、SCP をアタッチするすべてのアカウントで、アクセス許可が設定されたアクションを実行できなくなります。アクティブな AWS アクセスポータルセッションを使用して異なるアカウントに移動し、異なるロールを引き受けた場合でも、ユーザーのアクションはブロックされます。SCP によってユーザーのアクセスが完全にブロックされると、サインイン、割り当ての取り消し、および必要に応じて AWS アクセスポータルセッションを停止する機能を無効にできます。

SCPs を使用する代わりに、アクセス許可セットのインラインポリシーと、ユーザーがアクセスできるアクセス許可セットによって使用されるカスタマー管理ポリシーに拒否ポリシーを含めることもできます。

複数のユーザーのアクセスを取り消す必要がある場合は、条件ブロックの値のリストを使用できます。

```
        "Condition": {
                "StringEquals": {
                    "identitystore:userId": [" user1 userId", "user2 userId"...]
                    }
    }
```

> **Important**
>
> 使用する方法にかかわらず、他の是正措置を講じ、ユーザーのユーザー ID をポリシーに少なくとも 12 時間保持する必要があります。その後、ユーザーが引き受けたロールはすべて期限切れになり、拒否ポリシーからユーザー ID を削除できます。

リソースポリシー、Amazon EKS、および のアクセス許可セットの参照 AWS KMS

アクセス許可セットを AWS アカウントに割り当てると、IAM Identity Center は で始まる名前のロールを作成しますAWSReservedSSO_。

ロールのフルネームと Amazon リソースネーム (ARN) は、次の形式を使用します。

名前	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*

例えば、データベース管理者に AWS アカウントアクセスを許可するアクセス許可セットを作成すると、対応するロールが次の名前と ARN で作成されます。

名前	ARN
AWSReservedSSO_DatabaseAdministrator_1234567890abcdef	arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/

名前	ARN
	`eu-west-2/AWSReservedSSO_DatabaseAdministrator_1234567890abcdef`

AWS アカウントでこのアクセス許可セットへの割り当てをすべて削除すると、IAM Identity Center が作成した対応するロールも削除されます。後で同じ権限セットに新しい割り当てを行うと、IAM Identity Center はその権限セット用の新しいロールを作成します。新しいロールの名前と ARN には、異なる固有のサフィックスが含まれます。この例では、ユニークなサフィックスは「abcdef0123456789」です。

名前	ARN
`AWSReservedSSO_DatabaseAdministrator_` **`abcdef0123456789`**	`arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_DatabaseAdministrator_` **`abcdef0123456789`**

ロールの新しい名前と ARN のサフィックスを変更すると、元の名前と ARN を参照するポリシーはすべて になり out-of-date、対応するアクセス許可セットを使用する個人のアクセスが中断されます。たとえば、以下の設定で元の ARN が参照されている場合、ロールの ARN を変更すると、権限セットのユーザのアクセスが中断されます。

- Amazon Elastic Kubernetes Service (Amazon EKS) の `aws-auth ConfigMap` ファイル内
- AWS Key Management Service （ AWS KMS) キーのリソースベースのポリシー。このポリシーはキーポリシーとも呼ばれます。

ほとんどのサービスのリソースベースのポリシーを更新 AWS して、アクセス許可セットに対応するロールの新しい ARN を参照することはできますが、Amazon EKS の IAM で作成するバックアップロールと、ARN が変更され AWS KMS た場合は、バックアップロールが必要です。Amazon EKS では、バックアップ IAM ロールが `aws-auth ConfigMap` に存在している必要があります。 AWS KMSの場合、それはキーポリシーに存在しなければなりません。いずれの場合も、バックアップ IAM ロールがない場合は、 AWS Supportに連絡しなければなりません。

アクセスが中断されないようにするための推奨事項

権限セットに対応するロールの ARN の変更によるアクセスの中断を避けるため、次のことを行うことをお勧めします。

- 少なくとも 1 つの権限セット割り当てを維持します。

  この割り当ては、Amazon EKS `aws-auth ConfigMap`の で参照するロール、 のキーポリシー AWS KMS、または他の のリソースベースのポリシーを含む AWS アカウントで維持します AWS のサービス。

  例えば、`EKSAccess`アクセス許可セットを作成し、 AWS アカウント から対応するロール ARN を参照する場合`111122223333`、そのアカウントのアクセス許可セットに管理グループを完全に割り当てます。この割り当ては永続的であるため、IAM Identity Center は対応するロールを削除せず、名前を変更するリスクがなくなります。管理グループは、権限昇格のリスクなしにいつでもアクセスできます。
- Amazon EKS および の場合 AWS KMS: IAM で作成されたロールを含めます。

  Amazon EKS クラスタの `aws-auth ConfigMap` または AWS KMS キーのキーポリシーで、権限セットにロールの ARN を参照する場合、IAM で作成する少なくとも 1 つのロールも含めることを推奨します。ロールは、Amazon EKS クラスターへのアクセスまたは AWS KMS キーポリシーの管理を許可する必要があります。権限セットがこのロールを引き受けることができる必要があります。これにより、アクセス許可セットのロール ARN が変更された場合は、 `aws-auth ConfigMap`または AWS KMS キーポリシーで ARN への参照を更新できます。次のセクションでは、IAM で作成されたロールの信頼ポリシーを作成する方法の例を示します。このロールは `AdministratorAccess` 権限セットによってのみ引き受けることができます。

カスタム信頼ポリシーの例

以下は、IAM で作成されたロールへのアクセス`AdministratorAccess`許可セットを提供するカスタム信頼ポリシーの例です。この基盤を構成する主な要素には以下が含まれます。

- この信頼ポリシーのプリンシパル要素は、 AWS アカウントプリンシパルを指定します。このポリシーでは、アクセス`sts:AssumeRole`許可`111122223333`を持つ AWS アカウントのプリンシパルが、IAM で作成されたロールを引き受けることができます。
- このトラストポリシーの `Condition element` は、IAM で作成されたロールを引き受けるプリンシパルの追加要件を指定します。このポリシーでは、以下のロール ARN を持つ権限セットがロールを引き受けることができます。

```
arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/
AWSReservedSSO_AdministratorAccess_*"
```

> **Note**
>
> この Condition 要素には ArnLike 条件演算子が含まれ、権限セットロール ARN の末尾には固有のサフィックスではなくワイルドカードが使用されます。つまり、ポリシーは、アクセス許可セットのロール ARN が変更されても、IAM で作成されたロールを引き受けることをアクセス許可セットに許可します。

```
{
  "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_*"
        }
      }
    }
  ]
}
```

このようなポリシーに IAM で作成したロールを含めると、アクセス許可セットまたはアクセス許可セットへのすべての割り当てが誤って削除され、再作成された場合に AWS KMS keys、Amazon EKS クラスター、、またはその他の AWS リソースへの緊急アクセスが可能になります。

属性ベースのアクセスコントロール

属性ベースのアクセス制御 (ABAC) は、属性に基づいて権限を定義する認可戦略です。IAM Identity Center を使用して、任意の IAM Identity Center ID ソースから取得したユーザー属性 AWS アカウン

ト を使用して、複数の のリソースへのアクセス AWS を管理できます。では AWS、これらの属性はタグと呼ばれます。でユーザー属性 AWS をタグとして使用する AWS と、 できめ細かなアクセス許可を作成するプロセスが簡素化され、タグが一致する AWS リソースにのみワークフォースがアクセスできるようになります。

例えば、2 つの異なるチームに所属する開発者ボブとサリーを IAM Identity Center で同じアクセス権限セットに割り当て、アクセスコントロールにチーム名属性を選択することができます。Bob と Sally が にサインインすると AWS アカウント、IAM Identity Center は AWS セッションでチーム名属性を送信するため、Bob と Sally はチーム名属性が AWS プロジェクトリソースのチーム名タグと一致する場合にのみプロジェクトリソースにアクセスできます。将来、Bob が Sally のチームに移った場合、コーポレートディレクトリのチーム名属性を更新するだけで、Bob のアクセスを変更することができます。次回、ボブがサインインすると、 AWSでの権限の更新を必要とせず、自動的に新しいチームのプロジェクトリソースにアクセスできるようになります。

このアプローチは、IAM Identity Center で作成したり、管理しなければならない個別のパーミッションの数を減らすのにも役立ちます。これは、同じアクセス権限セットに関連付けられたユーザーが、その属性に基づいて独自の権限を持つことができるようになったためです。これらのユーザー属性を IAM Identity Center のアクセス許可セットとリソースベースのポリシーで使用して、 AWS リソースに ABAC を実装し、大規模なアクセス許可管理を簡素化できます。

利点

IAM Identity Center で ABAC を使用すると、以下のようなメリットがあります。

- ABAC では必要なアクセス権限セットの数が少ない - 職務ごとに異なるポリシーを作成する必要がないため、アクセス権限セットの数も少なくて済みます。これにより、許可管理の複雑さを軽減できます。
- ABAC を使用することで、チームは変化し、急速に成長することができる - リソースの作成時に適切なタグが付けられれば、属性に基づいて新しいリソースの権限が自動的に付与されます。
- ABAC で社内ディレクトリの従業員属性を利用する - IAM Identity Center で構成された任意の ID ソースから既存の従業員属性を使用して、 AWSでのアクセスコントロールの決定を行うことができます。
- リソースにアクセスしているユーザーを追跡する – セキュリティ管理者は、 のユーザー属性を確認して のユーザーアクティビティを追跡することで AWS CloudTrail 、セッションのアイデンティティを簡単に判断できます AWS。

IAM Identity Center コンソールを使って ABAC を設定する方法については、「アクセスコントロールの属性」を参照してください。IAM Identity Center APIs「」を参照してください。CreateInstanceAccessControlAttributeConfiguration

トピック

- チェックリスト: IAM Identity Center AWS を使用した での ABAC の設定
- アクセスコントロールの属性

チェックリスト: IAM Identity Center AWS を使用した での ABAC の設定

このチェックリストには、 AWS リソースを準備し、ABAC アクセス用の IAM Identity Center を設定するために必要な設定作業が含まれています。このチェックリストのタスクを順番に行います。リファレンスリンクからトピックに移動した場合は、このトピックに戻って、チェックリストの残りのタスクを引き続き行うことができます。

ステップ	タスク	リファレンス
1	すべての AWS リソースにタグを追加する方法を確認します。IAM Identity Center に ABAC を実装するには、まず、ABAC を実装したい AWS リソースすべてにタグを追加する必要があります。	• AWS リソースのタグ付け
2	IAM Identity Center の ID ソースを Identity Store で関連するユーザーの ID と属性で設定する方法を確認します。IAM Identity Center では、 で ABAC 用にサポートされている IAM Identity Center ID ソースのユーザー属性を使用できます AWS。	• ID ソースを管理する
3	以下の基準に基づいて、アクセスコントロールの決定に使用する属性を決定 AWS し、IAM Identity Center に送信します。	• 開始
	• 外部の ID プロバイダー (IdP) を使用している場合、IdP から渡された属性を使用するのか、それとも	• 外部 ID プロバイダーを ID ソースとして使用する際の属性を選択する

ステップ	タスク	リファレンス
	IAM Identity Center 内で属性を選択するのかを決定します。	
	• IdP に属性を送信させる場合は、SAML アサーションで属性を送信するように IdP を設定します。特定の IdP については`Optional`、チュートリアルのセクションを参照してください。	• 入門チュートリアル
	• ID ソースとして IdP を使用し、IAM Identity Center で属性を選択する場合は、属性値が IdP から来るように SCIM を構成する方法を調べます。IdP で SCIM を使用できない場合は、IAM Identity Center コンソールの [ユーザー] ページでユーザーとその属性を追加します。	• 自動プロビジョニング • サポートされている外部 ID プロバイダ属性
	• ID ソースとして Active Directory または IAM Identity Center を使用する場合、または IdP を使用して IAM Identity Center で属性を選択する場合は、設定可能な属性を確認してください。その後、すぐにステップ 4 に進み、IAM Identity Center コンソールを使って ABAC 属性の設定を開始します。	• IAM Identity Center を ID ソースとして使用する際の属性を選択する • AWS Managed Microsoft AD を ID ソースとして使用する際の属性を選択する • デフォルトのマッピング
4	IAM Identity Center コンソールの [アクセスコントロールの属性] ページで、ABAC に使用する属性を選択します。このページでは、ステップ 2 で設定した ID ソースから、アクセスコントロールのための属性を選択できます。ID とその属性が IAM Identity Center に保存されたら、キーと値のペア (マッピング) を作成して、アクセスコントロールの決定 AWS アカウント に使用する必要があります。	• アクセスコントロールのための属性の有効化と設定

ステップ	タスク	リファレンス
5	アクセス権限セット内にカスタム権限ポリシーを作成し、アクセスコントロール属性を使用して ABAC ルールを作成し、ユーザーが一致するタグを持つリソースにのみアクセスできるようにします。ステップ 4 で設定したユーザー属性は、 AWS のタグとしてアクセスコントロールの判断に使用されます。`aws:PrincipalTag/key` 条件を使用して、権限ポリシーのアクセスコントロール属性を参照することができます。	• IAM Identity Center を使用して ABAC の権限セットを作成する
6	さまざまな で AWS アカウント、ステップ 5 で作成したアクセス許可セットにユーザーを割り当てます。これにより、アカウントへのフェデレーションと AWS リソースへのアクセスが、一致するタグに基づいてのみ行われるようになります。	• へのユーザーアクセスを割り当てる AWS アカウント

これらのステップを完了すると、シングルサインオン AWS アカウント を使用して にフェデレーションするユーザーは、一致する属性に基づいて AWS リソースにアクセスできます。

アクセスコントロールの属性

[アクセスコントロールの属性] は、IAM Identity Center コンソールのページ名で、リソースへのアクセスコントロールをするためのポリシーで使用するユーザー属性を選択します。ユーザーの ID ソースの既存の属性 AWS に基づいて、 のワークロードにユーザーを割り当てることができます。

例えば、部署名に基づいて S3 バケットへのアクセスを割り当てたいとします。[Attributes for access control] (アクセスコントロールの属性)では、属性ベースのアクセスコントロール (ABAC) で使用する Department (部署) ユーザー属性を選択します。IAM Identity Center 権限セットでは、部署属性が、S3 バケットに割り当てた部門タグと一致した場合にのみ、ユーザーにアクセスを許可するポリシーを書き込みます。IAM Identity Center は、アクセスされるアカウントに、ユーザーの部門属性を渡します。そして、その属性は、ポリシーに基づいてアクセスを決定するために使用されます。ABAC の詳細については、「属性ベースのアクセスコントロール」を参照してください。

開始

アクセスコントロールの属性設定をどのように始めるかは、使用している ID ソースによって異なります。選択した ID ソースにかかわらず、属性を選択した後、アクセス権限セットのポリシーを作成または編集する必要があります。これらのポリシーは、ユーザーの ID に AWS リソースへのアクセスを許可する必要があります。

IAM Identity Center を ID ソースとして使用する際の属性を選択する

IAM Identity Center を ID ソースとして設定する場合、まずユーザーを追加し、その属性を設定します。次に、[Attributes for access control] (アクセスコントロールの属性) ページに移動して、ポリシーで使用する属性を選択します。最後に、AWS アカウントのページに移動して、ABAC の属性を使用するための権限セットを作成または編集します。

AWS Managed Microsoft AD を ID ソースとして使用する際の属性を選択する

IAM Identity Center をアイデンティティソース AWS Managed Microsoft AD として設定する場合、まず Active Directory から一連の属性を IAM Identity Center のユーザー属性にマッピングします。次に、[Attributes for access control] (アクセスコントロールの属性) のページに移動します。次に、アクティブディレクトリからマッピングされた既存の SSO 属性のセットに基づいて、ABAC 構成で使用する属性を選択します。最後に、アクセス権限セットに含まれるアクセスコントロール属性を用いて、 AWS リソースへのアクセスをユーザー ID に許可する ABAC ルールを作成します。IAM Identity Center のユーザー属性と AWS Managed Microsoft AD ディレクトリのユーザー属性のデフォルトマッピングのリストについては、「」を参照してくださいデフォルトのマッピング。

外部 ID プロバイダーを ID ソースとして使用する際の属性を選択する

外部 ID プロバイダー (IdP) を ID ソースとして IAM Identity Center を構成する場合、ABAC で属性を使用する方法は 2 つあります。

- SAML アサーションを通じて属性を送信するように IdP を設定することができます。この場合、IAM Identity Center はポリシー評価のために IdP から属性名と値を渡します。

> **Note**
>
> SAML アサーションの属性は、[Attributes for access control] (アクセスコントロールの属性) ページには表示されません。これらの属性を事前に把握しておき、ポリシー作成時にアクセスコントロールルールに追加する必要があります。属性 IdPs に対して外部を信頼する場合、ユーザーが にフェデレーションするときに、これらの属性は常に渡されます

AWS アカウント。同じ属性が SAML および SCIM を通じて IAM Identity Center に来る場合は、SAML の属性値がアクセスコントロールの決定において優先されます。

- どの属性を使用するかは、IAM Identity Center コンソールの [アクセスコントロールの属性] ページから設定できます。ここで選択した属性値は、アサーションを介して IdP から取得された値と一致する属性値に置き換えます。SCIM の使用状況に応じて、次のことを考慮してください。
  - SCIM を使用している場合、IdP は属性値を自動的に IAM Identity Center に同期させます。アクセスコントロールに必要な追加の属性は、SCIM 属性のリストに存在しない可能性があります。その場合、IdP の IT 管理者と協力して、必要な `https://aws.amazon.com/SAML/Attributes/AccessControl:` プレフィックスを使用した SAML アサーションを介して IAM Identity Center にそのような属性を送信することを検討してください。SAML アサーションを介して送信するように IdP でアクセスコントロールのユーザー属性を設定する方法については、IdP の入門チュートリアル「」を参照してください。
  - SCIM を使用しない場合は、IAM Identity Center を ID ソースとして使用する場合と同様に、手動でユーザーを追加し、属性を設定する必要があります。次に、[Attributes for access control] (アクセスコントロールの属性) ページに移動して、ポリシーで使用する属性を選択します。

IAM Identity Center のユーザー属性と外部 のユーザー属性でサポートされている属性の完全なリストについては IdPs、「」を参照してくださいサポートされている外部 ID プロバイダ属性。

IAM Identity Center で ABAC を使い始めるには、以下のトピックを参照してください。

トピック

- アクセスコントロールのための属性の有効化と設定
- IAM Identity Center を使用して ABAC の権限セットを作成する

アクセスコントロールのための属性の有効化と設定

すべてのケースで ABAC を使用するには、まず IAM Identity Center コンソールまたは IAM Identity Center API を使用して ABAC を有効にする必要があります。IAM Identity Center を使用して属性を選択する場合は、IAM Identity Center コンソールまたは IAM Identity Center API の「アクセスコントロール用の属性」ページを使用します。ID ソースとして外部 ID プロバイダ (IdP) を使用し、SAML アサーションを通じて属性を送信することを選択した場合、属性を渡すように IdP を構成します。SAML アサーションがこれらの属性のいずれかを渡した場合、IAM Identity Center はその属性値を IAM Identity Center ID ストアの値で置き換えます。ユーザーが自身のアカウントにフェデ

レーションする際に、アクセスコントロールの決定を行うため IAM Identity Center で構成された属性のみが送信されます。

> **Note**
>
> IAM Identity Center コンソールの [アクセスコントロールの属性] ページから、外部 IdP によって構成および送信された属性を表示することはできません。外部 IdP からの SAML アサーションでアクセスコントロール属性を渡している場合は、ユーザーがフェデレーションを行う際に、その属性が AWS アカウント に直接送信されます。その属性は IAM Identity Center でのマッピングには利用できません。

アクセスコントロールの属性を有効にする

IAM Identity Center コンソールを使用してアクセス属性 (ABAC) コントロール機能を有効にする場合は、次の手順で行います。

> **Note**
>
> 既存の権限セットがあり、IAM Identity Center インスタンスで ABAC を有効にする予定の場合、まず、追加のセキュリティ制限により、最初に `iam:UpdateAssumeRolePolicy` ポリシーを設定する必要があります。アカウントにアクセス権限セットを作成していない場合は、これらの追加のセキュリティ制限は必要ありません。

アクセスコントロールの属性を有効にする

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. [設定] ページで、[アクセス制御情報の属性] ボックスを探し、[有効化] を選択します。次の手順に進み、設定します。

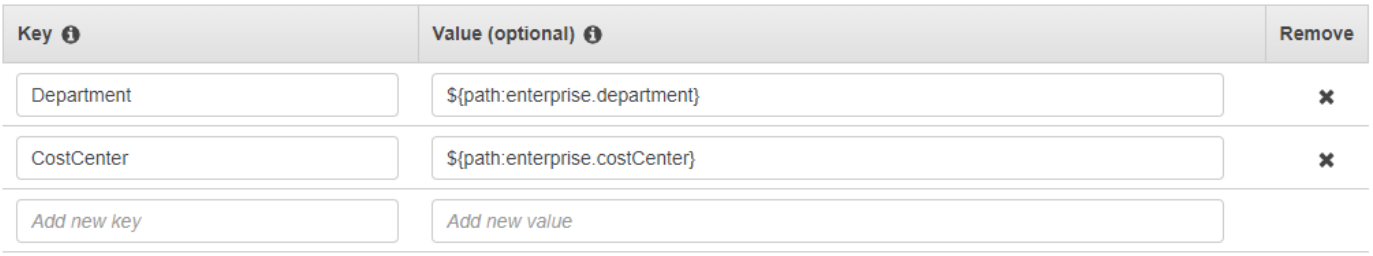
属性を選択します。

ABAC 構成の属性を設定は、次の手順で行います。

IAM Identity Center コンソールを使って属性を選択するには

1. IAM Identity Center コンソール を開きます。

2. [設定] を選択します。
3. [設定] ページで [アクセス制御用の属性] タブを選択し、[属性の管理] を選択します。
4. [アクセス制御の属性] ページで、[属性を追加] を選択し、[キー] と [値] の詳細を入力します。ここでは、ID ソースから送られてくる属性を、IAM Identity Center がセッションタグとして渡す属性にマッピングします。



キーは、ポリシーで使用するための属性に付ける名前を表します。これは任意の名前で構いませんが、アクセスコントロールのために作成したポリシーでは、その正確な名前を指定する必要があります。例えば、Okta (外部の IdP) を ID ソースとして使用しており、組織のコストセンターのデータをセッションタグとして渡す必要があるとします。キー には、キー名CostCenterと似た名前を入力します。重要なのは、ここでどのような名前を設定しても、`aws:PrincipalTag ####` (つまり `"ec2:ResourceTag/CostCenter": "${aws:PrincipalTag/CostCenter}"`) で、全く同じ名前を設定する必要があります。

> **Note**
>
> キーには単一値の属性 (例: **`Manager`**) を使用します。IAM Identity Center は ABAC の複数値属性 (例: **`Manager, IT Systems`**) をサポートしていません。

値は、設定された ID ソースから取得される属性のコンテンツを表します。ここでは、AWS Managed Microsoft AD　ディレクトリの属性マッピング にリストされている適切な ID ソーステーブルから任意の値を入力できます。例えば、上記の例では、サポートされている IdP 属性リストを確認して最も近い属性である **`${path:enterprise.costCenter}`** を特定し、それを値フィールドに入力します。上記のスクリーンショットを参考にしてください。SAML アサーションで属性を渡すオプションを使用しない限り、このリスト以外の外部 IdP の属性値を ABAC に使用することはできません。

5. [変更を保存] を選択します。

アクセスコントロール属性のマッピング設定できたので、ABAC 設定プロセスを完了させます。そのためには、ABAC ルールを作成し、権限セットやリソースベースのポリシーに追加します。これは、ユーザー ID に AWS リソースへのアクセスを許可するために必要です。詳細については、「IAM Identity Center を使用して ABAC の権限セットを作成する」を参照してください。

アクセスコントロールの属性を無効にする

次の手順で、ABAC 機能を無効にし、設定されていた属性マッピングをすべて削除します。

アクセスコントロールの属性を無効にする

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. [設定] ページで [アクセス制御用の属性] タブを選択し、[無効にする] を選択します。
4. [アクセス制御の属性を無効にする] ダイアログで情報を確認し、準備ができたら削除と入力し、[確認] を選択します。

> **Important**
>
> このステップでは、設定されていたすべての属性を削除します。削除すると、ID ソースから受信した属性や、以前に設定したカスタム属性は渡されません。

IAM Identity Center を使用して ABAC の権限セットを作成する

設定した属性値に基づいて AWS リソースにアクセスできるユーザーを決定するアクセス権限ポリシーを作成できます。ABAC を有効にして属性を指定すると、IAM Identity Center は認証されたユーザーの属性値を IAM に渡し、ポリシー評価で使用できるようにします。

aws:PrincipalTag 条件キー

アクセスコントロール属性は、アクセスコントロールルールを作成するための `aws:PrincipalTag` 条件キーを使って、アクセス権限セットに使用することができます。例えば、次の信頼ポリシーでは、組織内のすべてのリソースに、それぞれのコストセンターをタグ付けすることができます。また、開発者にコストセンターのリソースへのアクセスを許可する単一のアクセス権限セットを使用することもできます。これで、開発者が SSO とコストセンター属性を使ってアカウントに連携すると、それぞれのコストセンターのリソースにしかアクセスできなくなります。チームがプロジェクトに開発者やリソースを追加しても、リソースに正しいコストセンターをタグ付けするだけで済みます。次に、デベロッパーが AWS にフェデレーションするときに、セッションでコストセンター情報

を渡します AWS アカウント。その結果、組織がコストセンターに新しいリソースや開発者を追加しても、開発者は権限の更新を必要とせずに、コストセンターに整合したリソースを管理することができます。

```
{
    "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}"
                }
            }
        }
    ]
}
```

詳細については、「IAM ユーザーガイド」のaws:PrincipalTagおよび「EC2: 一致するプリンシパルタグとリソースタグに基づいてインスタンスを開始または停止する」を参照してください。

ポリシーの条件に無効な属性が含まれている場合、ポリシーの条件は失敗し、アクセスは拒否されます。詳細については、「ユーザーが外部の ID プロバイダーを使用してサインインしようとすると、「予期しないエラーが発生しました」というエラーが発生します」を参照してください。

IAM ID プロバイダー

にシングルサインオンアクセスを追加すると AWS アカウント、IAM Identity Center は各 に IAM ID プロバイダーを作成します AWS アカウント。IAM ID プロバイダーは、アクセスキーなどの長期的

セキュリティ認証情報をアプリケーションに配布したり組み込んだりする必要がないので、 AWS アカウント の安全性の維持に役立ちます。

IAM ID プロバイダーを修復する

ID プロバイダーを誤って削除または変更した場合は、ユーザーとグループの割り当てを手動で再適用する必要があります。ユーザーとグループの割り当てを再適用すると、ID プロバイダーが再作成されます。詳細については、以下を参照してください。

- へのアクセスを管理する AWS アカウント
- アプリケーションへのアクセスの管理

サービスリンクロール

サービスにリンクされたロールは、IAM Identity Center が、組織内の特定の AWS アカウント へのシングルサインオン· アクセスを持つユーザーを AWS Organizationsに委譲し、実施できるようにするための事前定義された権限を提供します。このサービスは、組織 AWS アカウント 内のすべての にサービスにリンクされたロールをプロビジョニングすることで、この機能を有効にします。その後、このサービスは、IAM Identity Center などの他の AWS サービスがそれらのロールを活用してサービス関連のタスクを実行できるようにします。詳細については、「AWS Organizations およびサービスにリンクされたロール」 を参照してください。

IAM Identity Center を有効にすると、IAM Identity Center は AWS Organizationsの組織内のすべてのアカウントにサ ービスにリンクされたロールを作成します。また、IAM Identity Center では、その後組織に追加されるすべてのアカウントに、同じサービスにリンクしたロールが作成されます。このロールは、IAM Identity Center が顧客に代わって各アカウントのリソースにアクセスすることを可能にします。詳細については、「へのアクセスを管理する AWS アカウント」を参照してください。

各 で作成されるサービスにリンクされたロール AWS アカウント には、 という名前が付けられますAWSServiceRoleForSSO。詳細については、「IAM Identity Center のサービスリンクロールの使用」を参照してください。

アプリケーションへのアクセスの管理

を使用すると AWS IAM Identity Center、アプリケーションへのシングルサインオンアクセス権を持つユーザーを制御できます。ユーザーは、ディレクトリの認証情報を使ってサインインすると、これらのアプリケーションにシームレスにアクセスできます。

IAM Identity Center は、IAM Identity Center とアプリケーションのサービスプロバイダーとの間の信頼関係を介して、これらのアプリケーションと安全にやり取りします。この信頼は、アプリケーションの種類に応じてさまざまな方法で作成できます。

IAM Identity Center は、AWS マネージドアプリケーションとカスタマーマネージドアプリケーションの 2 つのアプリケーションタイプをサポートしています。 AWS マネージドアプリケーションは、関連するアプリケーションコンソール内から直接、またはアプリケーション APIsを介して設定されます。カスタマーマネージドアプリケーションは、IAM アイデンティティセンターコンソールに追加され、IAM アイデンティティセンターおよびサービスプロバイダーの両方で適切なメタデータを設定する必要があります。

IAM アイデンティティセンターと連携するようにアプリケーションを設定すると、そのアプリケーションにアクセスするユーザーまたはグループを管理できます。デフォルトでは、ユーザーはアプリケーションに割り当てられません。

また、組織 AWS アカウント 内の特定の AWS Management Console の へのアクセス権を従業員に付与することもできます。詳細については、「へのアクセスを管理する AWS アカウント」を参照してください。

トピック

- AWS マネージドアプリケーション
- カスタマーマネージドアプリケーション
- アプリケーション間での信頼されたアイデンティティのプロパゲーション
- IAM Identity Center 証明書の管理
- IAM アイデンティティセンターコンソールのアプリケーションプロパティを設定する
- IAM Identity Center コンソールでアプリケーションへのユーザーアクセスを割り当てます。
- IAM Identity Center コンソールでユーザーアクセスを削除します。
- アプリケーションの属性を IAM Identity Center の属性にマップする

AWS マネージドアプリケーション

AWS マネージドアプリケーションは IAM Identity Center と統合され、認証およびディレクトリサービスに使用できます。

AWS マネージドアプリケーションを IAM Identity Center と統合することで、アプリケーションごとに個別のフェデレーションやユーザーとグループの同期を設定することなく、ユーザーアクセスを簡単に割り当てることができます。認証に使用する ID ソースを 1 回接続すると、ユーザーとグループの割り当てが 1 つのビューに表示されます。信頼できる ID の伝播を有効にするアプリケーションの管理者は、ユーザーまたはユーザーのグループメンバーシップに基づいてアプリケーションリソースへのアクセスを定義および監査できます。IAM ロールにマッピングする必要はありません。

AWS マネージドアプリケーションは、アプリケーションリソースへのアクセスを管理するために使用できる管理ユーザーインターフェイスを提供します。例えば、 QuickSight 管理者はグループメンバーシップに基づいてダッシュボードにアクセスするユーザーを割り当てることができます。ほとんどの AWS マネージドアプリケーションは、アプリケーションにユーザーを割り当てるための AWS Management Console エクスペリエンスも提供します。これらのアプリケーションのコンソール環境には、ユーザー割り当て機能とアプリケーションリソースへのアクセスを管理する機能を組み合わせるために、両方の機能が統合されている場合があります。

AWS IAM Identity Center と統合された マネージドアプリケーションには、次のものがあります。

AWS IAM Identity Center と統合する マネージドアプリケーション

AWS マネージドアプリケーション	IAM Identity Center の組織インスタンスと統合	IAM Identity Center のアカウントインスタンスと統合	IAM Identity Center を介した信頼できる ID の伝播を有効にする
Amazon Athena SQL	 はい	 はい	 はい
Amazon CodeCatalyst	 はい	 はい	 いいえ

AWS マネージドアプリケーション	IAM Identity Center の組織インスタンスと統合	IAM Identity Center のアカウントインスタンスと統合	IAM Identity Center を介した信頼できる ID の伝播を有効にする
Amazon EMR ノートブック	はい	いいえ	いいえ
Amazon EC2 での Amazon EMR	はい	はい	はい
Amazon EMR Studio	はい	はい	はい
Amazon Kendra	はい	いいえ	いいえ
Amazon Managed Grafana	はい	いいえ	いいえ
Amazon Monitron	はい	いいえ	いいえ

AWS マネージドアプリケーション	IAM Identity Center の組織インスタンスと統合	IAM Identity Center のアカウントインスタンスと統合	IAM Identity Center を介した信頼できる ID の伝播を有効にする
Amazon Nimble Studio	はい	いいえ	いいえ
Amazon Pinpoint	はい	いいえ	いいえ
Amazon Q Business	はい	はい	いいえ
Amazon Q Developer	はい	はい *	いいえ
Amazon QuickSight	はい	はい	はい
Amazon Redshift	はい	はい	はい

AWS マネージドアプリケーション	IAM Identity Center の組織インスタンスと統合	IAM Identity Center のアカウントインスタンスと統合	IAM Identity Center を介した信頼できる ID の伝播を有効にする
Amazon S3 Access Grants	はい	はい	はい
Amazon SageMaker Studio	はい	いいえ	いいえ
Amazon WorkSpaces Web	はい	いいえ	いいえ
AWS CLI	はい	いいえ	いいえ
AWS Deadline Cloud	はい	はい	いいえ
AWS IoT Events	はい	いいえ	いいえ

AWS マネージドアプリケーション	IAM Identity Center の組織インスタンスと統合	IAM Identity Center のアカウントインスタンスと統合	IAM Identity Center を介した信頼できる ID の伝播を有効にする
AWS IoT Fleet Hub	はい	いいえ	いいえ
AWS IoT SiteWise	はい	いいえ	いいえ
AWS Lake Formation	はい	はい	はい
AWS Supply Chain	はい	いいえ	いいえ
AWS Systems Manager	はい	いいえ	いいえ
AWS Verified Access	はい	いいえ	いいえ

* IAM Identity Center のアカウントインスタンスは、ユーザーがコンソールで Amazon Q にアクセスする必要がある場合を除き、サポートされます AWS 。

トピック

アクセスの制御

AWS マネージドアプリケーションへのアクセスは、次の 2 つの方法で制御されます。

- アプリケーションへの初回入力 — IAM アイデンティティセンターは、アプリケーションへの割り当てを通じてこれを管理します。デフォルトでは、 AWS マネージドアプリケーションには割り当てが必要です。
- アプリケーションリソースへのアクセス — アプリケーションは、自身が制御する独立したリソース割り当てを通じてこれを管理します。

管理タスクの調整

アプリケーション管理者である場合、アプリケーションへの割り当てを必須にするかどうかを選択できます。割り当てが必要な場合、ユーザーが AWS アクセスポータルにサインインすると、アプリケーションに直接割り当てられたユーザー、またはグループ割り当てによって割り当てられたユーザーのみがアプリケーションタイルを表示できます。また、割り当てが不要な場合は、すべての IAM アイデンティティセンターユーザーがアプリケーションにアクセスできるようにすることができます。この場合、アプリケーションは リソースへのアクセスを管理し、アプリケーションタイルは AWS アクセスポータルにアクセスするすべてのユーザーに表示されます。

IAM Identity Center 管理者の場合は、IAM Identity Center コンソールを使用して、 AWS マネージドアプリケーションへの割り当てを削除できます。割り当てを削除する前に、アプリケーション管理者

と調整することをお勧めします。また、割り当てが必要かどうかを決定する設定を変更したり、アプリケーションの割り当てを自動化したりする予定がある場合は、アプリケーション管理者と調整する必要があります。

ID 情報を共有するための IAM アイデンティティセンターの設定

IAM アイデンティティセンターは、サインイン認証情報を除く、ユーザーおよびグループの属性を含む ID ストアを提供します。以下のいずれかの方法で、IAM Identity Center ID ストアのユーザーとグループを更新することができます。

- IAM Identity Center ID ストアをメインの ID ソースとして使用します。この方法を選択した場合は、IAM Identity Center コンソールまたは AWS Command Line Interface () 内からユーザー、そのサインイン認証情報、およびグループを管理しますAWS CLI。詳細については、「IAM Identity Center で ID を管理する」を参照してください。
- 以下のいずれかの ID ソースから IAM Identity Center の ID ストアにユーザーとグループのプロビジョニング (同期) を設定します。
  - Active Directory - 詳細については、「Microsoft AD ディレクトリへの接続」を参照してください。
  - 外部 ID プロバイダー - 詳細については、「外部 ID プロバイダに接続する方法には」を参照してください。

  このプロビジョニング方法を選択した場合、ユーザーとグループの管理は ID ソース内で継続され、それらの変更は IAM アイデンティティセンターの ID ストアに同期されます。

どの ID ソースを選択しても、IAM Identity Center はユーザーおよびグループの情報を AWS マネージドアプリケーションと共有できます。そのように、ID ソースを一度 IAM アイデンティティセンターに接続するだけで、 AWS クラウド内の複数のアプリケーションで ID 情報を共有することが可能になります。これにより、アプリケーションごとにフェデレーションや ID のプロビジョニングを個別に設定する必要がなくなります。また、この共有機能により、ユーザーに別の AWS アカウントで、多数のアプリケーションへのアクセスを簡単に与えることができます。

で ID 情報を共有する際の考慮事項 AWS アカウント

IAM アイデンティティセンターは、アプリケーション全体で最もよく使用される属性をサポートします。これらの属性には、姓名、電話番号、E メールアドレス、住所、優先する言語が含まれます。この個人を特定できる情報を使用できるアプリケーションとアカウントを慎重に検討してください。

この情報へのアクセスは、次のいずれかの方法で制御できます。 AWS Organizations 管理アカウントのみ、または のすべてのアカウントでアクセスを有効にすることができます AWS Organizations。あるいは、サービスコントロールポリシーを使って、どのアプリケーションが、AWS Organizationsのどのアカウントの情報にアクセスできるかを制御することができます。例えば、 AWS Organizations 管理アカウントでのみアクセスを有効にすると、メンバーアカウントのアプリケーションは情報にアクセスできなくなります。すべてのアカウントでアクセスを有効にすると、SCP を使用して許可するアプリケーションを除く、すべてのアプリケーションによるアクセスを禁止できます。

ID 対応コンソールセッションの有効化

コンソールのアイデンティティ対応セッションは、ユーザーのエクスペリエンスをパーソナライズするための追加のユーザーコンテキストを提供することで、ユーザーの AWS コンソールセッションを強化します。この機能は現在、 コンソールで Amazon Q のユーザーに対してサポートされています AWS 。

アイデンティティ対応のコンソールセッションは、既存のアクセスパターンや AWS コンソールへのフェデレーションを今すぐ変更することなく有効にできます。ユーザーが IAM で AWS コンソールにサインインする場合 (例えば、IAM ユーザーとしてサインインする場合や、IAM とのフェデレーションアクセスを通じてサインインする場合) 、これらのメソッドを引き続き使用できます。ユーザーが AWS アクセスポータルにサインインすると、IAM Identity Center のユーザー認証情報を引き続き使用できます。

トピック

前提条件と考慮事項

ID 対応コンソールセッションを有効にする前に、以下の前提条件と考慮事項を確認してください。

- コンソールで Amazon Q へのアクセスを必要とするユーザーに対して、アイデンティティ対応の AWS コンソールセッションを有効にする必要があります。
- ID 対応コンソールセッションは現在、 AWS コンソールの Amazon Q でのみサポートされています。
- ID 対応コンソールセッションには、IAM Identity Center の組織インスタンスが必要です。

- オプトイン で IAM Identity Center を有効にした場合、Amazon Q との統合はサポートされていません AWS リージョン。
- ID 対応コンソールセッションを有効にした後は、この機能を無効にすることはできません。
- ID 対応コンソールセッションを有効にするには、次のアクセス許可が必要です。
  - `sso:CreateApplication`
  - `sso:GetSharedSsoConfiguration`
  - `sso:ListApplications`
  - `sso:PutApplicationAssignmentConfiguration`
  - `sso:PutApplicationAuthenticationMethod`
  - `sso:PutApplicationGrant`
  - `sso:PutApplicationAccessScope`
  - `signin:CreateTrustedIdentityPropagationApplicationForConsole`
  - `signin:ListTrustedIdentityPropagationApplicationForConsole`
  -
- ユーザーがアイデンティティ対応コンソールセッションを使用できるようにするには、アイデンティティベースのポリシーで `sts:setContext` 許可を付与する必要があります。詳細については、「ID 対応コンソールセッションを使用するアクセス許可をユーザーに付与する」を参照してください。

identity-aware-console セッションを有効にする方法

ID 対応コンソールセッションは、Amazon Q コンソールまたは IAM Identity Center コンソールで有効にできます。

Amazon Q コンソールでアイデンティティ対応コンソールセッションを有効にする

ID 対応コンソールセッションを有効にする前に、ID ソースが接続された IAM Identity Center の組織インスタンスが必要です。IAM Identity Center を既に設定している場合は、ステップ 3 に進みます。

1. IAM Identity Center コンソールを開きます。を有効化を選択し、IAM Identity Center の組織インスタンスを作成します。詳細については、「の有効化 AWS IAM Identity Center」を参照してください。
2. ID ソースを IAM Identity Center に接続し、ユーザーを IAM Identity Center にプロビジョニングします。デフォルトの IAM Identity Center ディレクトリを ID ソースとして選択することも、別

の ID プロバイダーを使用することもできます。詳細については、「入門チュートリアル」を参照してください。

3. IAM Identity Center の設定が完了したら、Amazon Q コンソールを開き、「Amazon Q デベロッパーユーザーガイド」の「サブスクリプション」の手順に従います。ID 対応コンソールセッションを必ず有効にしてください。

> **Note**
>
> ID 対応コンソールセッションを有効にするための十分なアクセス許可がない場合は、IAM Identity Center コンソールでこのタスクを実行するように IAM Identity Center 管理者に依頼する必要がある場合があります。詳細については、次の手順を参照してください。

IAM Identity Center コンソールでアイデンティティ対応コンソールセッションを有効にする

IAM Identity Center 管理者の場合、IAM Identity Center コンソールでアイデンティティ対応コンソールセッションを有効にするように別の管理者から求められることがあります。

1. IAM Identity Center コンソールを開きます。
2. ナビゲーションペインで [設定] を選択します。
3. ID 対応セッションを有効にする で、 を有効にする を選択します。
4. 2 番目のメッセージで、 を有効にするを選択します。
5. ID 対応コンソールセッションの有効化が完了すると、設定ページの上部に確認メッセージが表示されます。
6. 詳細 セクションでは、アイデンティティ対応セッションのステータスは有効 です。

ID 対応コンソールセッションの仕組み

ID 対応のコンソールセッションを使用すると、 AWS コンソールの Amazon Q のユーザーは にサインインし AWS、 AWS Management Console または他の AWS ウェブサイトを開き、Amazon Q アイコンを選択し、チャットを開始したり、サポートされている他の機能を使用したりできます。詳細については、「Amazon Q Developer ユーザーガイド」を参照してください。

IAM Identity Center は、ユーザーの現在のコンソールセッションを強化して、アクティブな IAM Identity Center ユーザーの ID と IAM Identity Center セッション ID を含めます。

アイデンティティ対応コンソールセッションには、次の 3 つの値が含まれます。

- Identity Store ユーザー ID (ID ストア：UserId) - この値は、IAM Identity Center に接続されている ID ソース内のユーザーを一意に識別するために使用されます。
- アイデンティティストアディレクトリ ARN (ID ストア：IdentityStoreArn) - この値は、IAM Identity Center に接続されているアイデンティティストアの ARN であり、 の属性を検索できますidentitystore:UserId。
- IAM Identity Center セッション ID - この値は、ユーザーの IAM Identity Center セッションがまだ有効かどうかを示します。

値は同じですが、ユーザーがサインインする方法に応じて、さまざまな方法で取得され、プロセスのさまざまな時点で追加されます。

- IAM Identity Center (AWS アクセスポータル) : この場合、ユーザーの ID ストアのユーザー ID と ARN 値は、アクティブな IAM Identity Center セッションで既に指定されています。IAM Identity Center は、セッション ID のみを追加することで現在のセッションを強化します。
- その他のサインイン方法 : ユーザーが IAM ユーザー AWS 、IAM ロール、または IAM のフェデレーティッドユーザーとして にサインインする場合、これらの値は提供されません。IAM Identity Center は、ID ストアユーザー ID、ID ストアディレクトリ ARN、およびセッション ID を追加することで、現在のセッションを強化します。

AWS マネージドアプリケーションの使用を制限する

IAM Identity Center を初めて有効にすると、 AWS では、 のすべてのアカウントで AWS マネージドアプリケーションを自動的に使用できます AWS Organizations。アプリケーションを制約するには、SCP を実装する必要があります。SCP を使用して、IAM アイデンティティセンターのユーザーおよびグループ情報へのアクセスをブロックし、指定したアカウント以外ではアプリケーションを起動できないようにすることができます。

AWS マネージドアプリケーションに関する詳細の表示

コンソールまたはアプリケーションの APIs を使用して AWS マネージドアプリケーションを IAM Identity Center に接続すると、アプリケーションは IAM Identity Center に登録されます。アプリケーションが IAM アイデンティティセンターに登録されると、IAM アイデンティティセンターコンソールでアプリケーションに関する詳細情報を表示できます。

IAM Identity Center コンソールで AWS マネージドアプリケーションに関する情報を表示するには

1. IAM Identity Center コンソール を開きます。
2. [Applications] (アプリケーション) を選択します。
3. [AWS マネージドアプリケーション] タブを選択します。
4. アプリケーションのリストで、詳細情報を表示するアプリケーションの名前を選択します。
5. アプリケーションに関する情報には、ユーザーとグループの割り当てが必要かどうか、該当する場合は ID を伝播するために割り当てられたユーザーとグループ、および信頼できるアプリケーションが含まれます。信頼できる ID 伝播の詳細については、「アプリケーション間での信頼されたアイデンティティのプロパゲーション」を参照してください。

AWS マネージドアプリケーションの無効化

ユーザーが AWS マネージドアプリケーションに対して認証されないようにするには、IAM Identity Center コンソールでアプリケーションを無効にします。

> **Warning**
>
> アプリケーションを無効にすることにより、このアプリケーションに対するすべてのユーザーアクセス許可を削除し、アプリケーションを IAM アイデンティティセンターから切り離し、アプリケーションにアクセスできないようにします。IAM アイデンティティセンター管理者である場合は、このタスクを実行する前にアプリケーション管理者と調整することをお勧めします。

AWS マネージドアプリケーションを無効にするには

1. IAM Identity Center コンソール を開きます。
2. [Applications] (アプリケーション) を選択します。
3. [アプリケーション] ページの [AWS マネージドアプリケーション] で、無効にするアプリケーションを選択します。
4. アプリケーションを選択した状態で、[アクション] を選択し、[無効にする] を選択します。
5. [アプリケーションの中断] ダイアログで、[中断] を選択します。
6. [AWS マネージドアプリケーション] リストでは、アプリケーションの状態は [非アクティブ」と表示されます。

カスタマーマネージドアプリケーション

IAM Identity Center を使用すると、ワークフォースユーザーを作成または接続し、すべての AWS アカウント およびアプリケーションへのアクセスを一元管理できます。IAM アイデンティティセンターは中央の ID サービスとして機能し、ユーザーを認証するためのさまざまな方法を提供します。すでに ID プロバイダー (IdP) を使用している場合は、IAM アイデンティティセンターを IdP と統合して、ユーザーとグループを IAM アイデンティティセンターにプロビジョニングし、ご自分の IdP を認証に使用することができます。

SAML 2.0 をサポートするカスタマーマネージドアプリケーションを使用している場合は、SAML 2.0 を介して IdP を IAM アイデンティティセンターにフェデレーションし、IAM アイデンティティセンターを使用してそれらのアプリケーションへのユーザーアクセスを管理できます。IAM アイデンティティセンターには、Salesforce や Microsoft 365 など、SAML 2.0 をサポートする一般的に使用されるアプリケーションのカタログが用意されています。このカタログは IAM Identity Center コンソールで使用できます。独自の SAML 2.0 アプリケーションを設定することもできます。

> **Note**
>
> OAuth 2.0 をサポートするカスタマーマネージドアプリケーションがあり、ユーザーがこれらのアプリケーションから AWS サービスにアクセスする必要がある場合は、信頼できる ID の伝播を使用できます。信頼できる ID の伝播を使用すると、ユーザーはアプリケーションにサインインでき、そのアプリケーションは AWS サービスのデータにアクセスするためのリクエストでユーザーの ID を渡すことができます。詳細については、「カスタマーマネージドアプリケーションによる信頼できる ID の伝播の使用」を参照してください。

トピック

- SAML 2.0 と OAuth 2.0
- カスタマー管理 SAML 2.0 アプリケーションの設定

SAML 2.0 と OAuth 2.0

IAM アイデンティティセンターでは、SAML 2.0 アプリケーションまたは OAuth 2.0 アプリケーションへのシングルサインオンアクセスをユーザーに提供できます。以下のトピックでは、SAML 2.0 と OAuth 2.0 の大まかな概観を説明します。

トピック

- SAML 2.0
- OAuth 2.0

SAML 2.0

SAML 2.0 は、SAML 認証機関 (ID プロバイダーまたは IdP) と SAML 2.0 コンシューマー (サービスプロバイダーまたは SP) との間でユーザーに関する情報を渡す SAML アサーションを安全に交換するための業界標準です。IAM Identity Center は、この情報を使用して、 アクセスポータル内のアプリケーションの使用を許可されたユーザーにフェデレーティッドシングルサインオン AWS アクセスを提供します。

OAuth 2.0

OAuth 2.0 は、アプリケーションがパスワードを共有せずにユーザーデータに安全にアクセスして共有できるようにするプロトコルです。この機能により、アプリケーションによるリソースへのアクセスを、安全かつ標準化された方法でユーザーに許可できます。アクセスは、さまざまな OAuth 2.0 付与フローによって容易になります。

IAM Identity Center を使用すると、パブリッククライアントで実行されるアプリケーションは、ユーザーに代わってプログラムで AWS アカウント および のサービスにアクセスするための一時的な認証情報を取得できます。パブリッククライアントは通常、ローカルでアプリケーションを実行するために使用されるデスクトップ、ラップトップ、またはその他のモバイルデバイスです。パブリッククライアントで実行される AWS アプリケーションの例としては、 AWS Command Line Interface（ AWS CLI ）AWS Toolkit、、 AWS Software Development Kits (SDKs。これらのアプリケーションが認証情報を取得できるようにするために、IAM Identity Center は次の OAuth 2.0 フローの一部をサポートしています。

- コード交換 (PKCE) の証明キーを使用した認証コードの付与 (RFC 6749 および RFC 7636)
- デバイス認証付与 (RFC 8628)

> **Note**
>
> これらのグラントタイプは、この機能をサポートする AWS のサービス でのみ使用できます。これらのサービスは、すべての でこの付与タイプをサポートしているとは限りません AWS リージョン。リージョンの違い AWS のサービス については、関連する のドキュメントを参照してください。

OpenID Connect (OIDC) は、OAuth 2.0 Framework に基づく認証プロトコルです。OIDC は、認証に OAuth 2.0 を使用する方法を指定します。IAM Identity Center OIDC サービス APIs を通じて、アプリケーションは OAuth 2.0 クライアントを登録し、これらのフローのいずれかを使用して、IAM Identity Center で保護された APIs にアクセス許可を付与するアクセストークンを取得します。アプリケーションは、目的の API ユーザーを宣言するためのアクセススコープを指定します。IAM Identity Center 管理者として ID ソースを設定した後、アプリケーションのエンドユーザーがまだサインインプロセスを完了していない場合は、サインインプロセスを完了する必要があります。その後、エンドユーザーは、アプリケーションが API コールを行うことを許可することに同意する必要があります。これらの API コールは、ユーザーのアクセス許可を使用して行われます。これに応じて、IAM Identity Center は、ユーザーが同意したアクセススコープを含むアクセストークンをアプリケーションに返します。

OAuth 2.0 許可フローの使用

OAuth 2.0 グラントフローは、フローをサポートする AWS マネージドアプリケーションでのみ使用できます。OAuth 2.0 フローを使用するには、IAM Identity Center のインスタンスと、使用するサポートされている AWS マネージドアプリケーションのインスタンスを単一の にデプロイする必要があります AWS リージョン。各 のドキュメントを参照して AWS のサービス 、 AWS マネージドアプリケーションのリージョンでの可用性と、使用する IAM Identity Center のインスタンスを確認してください。

OAuth 2.0 フローを使用するアプリケーションを使用するには、エンドユーザーはアプリケーションが接続して IAM Identity Center のインスタンスに登録する URL を入力する必要があります。アプリケーションに応じて、管理者として、IAM Identity Center のインスタンスのAWS アクセスポータル URL または発行者 URL をユーザーに提供する必要があります。これら 2 つの設定は、IAM Identity Center コンソールの設定ページで確認できます。クライアントアプリケーションの設定の詳細については、そのアプリケーションのドキュメントを参照してください。

アプリケーションにサインインして同意するためのエンドユーザーエクスペリエンスは、アプリケーションが PKCE を使用した認可コード付与または を使用しているかどうかによって異なりますデバイス認証付与。

PKCE を使用した認可コード付与

このフローは、ブラウザのあるデバイスで実行されるアプリケーションによって使用されます。

1. ブラウザウィンドウが開きます。
2. ユーザーが認証されていない場合、ブラウザはユーザー認証を完了するようにリダイレクトします。

3. 認証後、ユーザーに次の情報を表示する同意画面が表示されます。
   - アプリケーションの名前
   - アプリケーションが使用の同意をリクエストしているアクセススコープ
4. ユーザーは同意プロセスをキャンセルすることも、同意して、ユーザーのアクセス許可に基づいてアプリケーションがアクセスを続行することもできます。

デバイス認証付与

このフローは、ブラウザの有無にかかわらずデバイスで実行されるアプリケーションで使用できます。アプリケーションがフローを開始すると、アプリケーションは URL とユーザーコードを提示し、ユーザーはフローの後半で検証する必要があります。フローを開始するアプリケーションが、ユーザーが同意したデバイスとは異なるデバイスで実行されている可能性があるため、ユーザーコードが必要です。このコードにより、ユーザーは他のデバイスで開始したフローに同意したことになります。

1. ブラウザを使用してデバイスからフローが開始されると、ブラウザウィンドウが開きます。フローがブラウザのないデバイスから開始された場合、ユーザーは別のデバイスでブラウザを開き、アプリケーションが提示した URL に移動する必要があります。
2. いずれの場合も、ユーザーが認証されていない場合、ブラウザはユーザー認証を完了するようにリダイレクトします。
3. 認証後、ユーザーに次の情報を表示する同意画面が表示されます。
   - アプリケーションの名前
   - アプリケーションが使用の同意をリクエストしているアクセススコープ
   - アプリケーションがユーザーに提示したユーザーコード
4. ユーザーは同意プロセスをキャンセルすることも、同意して、ユーザーのアクセス許可に基づいてアプリケーションがアクセスを続行することもできます。

アクセススコープ

スコープは、OAuth 2.0 フローを介してアクセスできるサービスのアクセスを定義します。スコープは、リソースサーバーとも呼ばれるサービスが、アクションとサービスリソースに関連するアクセス許可をグループ化する方法であり、OAuth 2.0 クライアントがリクエストできる粗粒度のオペレーションを指定します。OAuth 2.0 クライアントが IAM Identity Center OIDC サービスに登録すると、クライアントは意図したアクションを宣言するスコープを指定します。そのためには、ユーザーが同意する必要があります。

OAuth 2.0 クライアントは、OAuth 2.0 (RFC 6749) のセクション 3.3 で定義されているscope値を使用して、アクセストークンに対してリクエストされるアクセス許可を指定します。クライアントは、アクセストークンをリクエストするときに最大 25 個のスコープを指定できます。PKCE または Device Authorization Grant フローで認証コード付与中にユーザーが同意すると、IAM Identity Center はスコープを返すアクセストークンにエンコードします。

AWS は、サポートされている のスコープを IAM Identity Center に追加します AWS のサービス。次の表は、パブリッククライアントを登録するときに IAM Identity Center OIDC サービスがサポートするスコープの一覧です。

パブリッククライアントの登録時に IAM Identity Center OIDC サービスがサポートするアクセススコープ

スコープ	説明	がサポートするサービス
`sso:account:access`	IAM Identity Center が管理するアカウントとアクセス権限セットにアクセスします。	IAM アイデンティティセンター
`codewhisperer:analysis`	Amazon Q デベロッパーコード分析へのアクセスを有効にします。	AWS ビルダー ID および IAM Identity Center
`codewhisperer:completions`	Amazon Q インラインコードの提案へのアクセスを有効にします。	AWS ビルダー ID および IAM Identity Center
`codewhisperer:conversations`	Amazon Q チャットへのアクセスを有効にします。	AWS ビルダー ID および IAM Identity Center
`codewhisperer:taskassist`	ソフトウェア開発のために Amazon Q デベロッパーエージェントへのアクセスを有効にします。	AWS ビルダー ID および IAM Identity Center
`codewhisperer:transformations`	コード変換のために Amazon Q デベロッパーエージェントへのアクセスを有効にします。	AWS ビルダー ID および IAM Identity Center

スコープ	説明	がサポートするサービス
`codecatalyst:read_write`	Amazon CodeCatalyst リソースの読み取りと書き込みを行い、既存のすべてのリソースへのアクセスを許可します。	AWS ビルダー ID および IAM Identity Center

カスタマー管理 SAML 2.0 アプリケーションの設定

SAML 2.0 をサポートするカスタマーマネージドアプリケーションを使用している場合は、SAML 2.0 を介して IdP を IAM アイデンティティセンターにフェデレーションし、IAM アイデンティティセンターを使用してそれらのアプリケーションへのユーザーアクセスを管理できます。IAM アイデンティティセンターコンソールでよく使用されるアプリケーションのカタログから SAML 2.0 アプリケーションを選択するか、独自の SAML 2.0 アプリケーションを設定できます。

> **Note**
>
> OAuth 2.0 をサポートするカスタマーマネージドアプリケーションがあり、ユーザーがこれらのアプリケーションから AWS サービスにアクセスする必要がある場合は、信頼できる ID の伝播を使用できます。信頼できる ID の伝播を使用すると、ユーザーはアプリケーションにサインインでき、そのアプリケーションは AWS サービスのデータにアクセスするためのリクエストでユーザーの ID を渡すことができます。詳細については、「カスタマーマネージドアプリケーションによる信頼できる ID の伝播の使用」を参照してください。

トピック

- IAM アイデンティティセンターアプリケーションカタログ
- 独自の SAML 2.0 アプリケーションをセットアップする

IAM アイデンティティセンターアプリケーションカタログ

IAM アイデンティティセンターコンソールのアプリケーションカタログを使用して、IAM アイデンティティセンターと連携するよく使用されている多くの SAML 2.0 アプリケーションを追加することができます。例としては、Salesforce、Box、Microsoft 365 などがあります。

ほとんどのアプリケーションで、IAM アイデンティティセンターとアプリケーションのサービスプロバイダーとの間の信頼関係を設定する方法に関する詳細情報が提供されます。この情報は、カタ

ログでアプリケーションを選択すると、アプリケーションの設定ページで利用できます。アプリケーションを設定したら、必要に応じて IAM アイデンティティセンターのユーザーまたはグループにアクセス権を割り当てることができます。

トピック

- アプリケーションカタログからアプリケーションをセットアップする

アプリケーションカタログからアプリケーションをセットアップする

IAM アイデンティティセンターとアプリケーションのサービスプロバイダーとの間で SAML 2.0 の信頼関係を設定するには、以下の手順を実行します。

この手順を開始する前に、信頼をより効率的に設定できるように、サービスプロバイダーのメタデータ交換ファイルがあることが役に立ちます。このファイルがない場合でも、まだこの手順を使用してその信頼を手動で設定できます。

アプリケーションカタログからアプリケーションを追加および設定するには

1. IAM Identity Center コンソール を開きます。
2. [Applications] (アプリケーション) を選択します。
3. [カスタマーマネージド] タブを選択します。
4. [アプリケーションの追加] を選択します。
5. [アプリケーションタイプを選択] ページの [セットアッププリファレンス] で、[カタログからアプリケーションを選択したい] を選択します。
6. [アプリケーションカタログ] で、追加するアプリケーションの名前を検索ボックスに入力し始めます。
7. 検索結果に表示されたら、一覧からアプリケーションの名前を選択し、[次へ] を選択します。
8. [アプリケーションを設定] ページの [表示名] と [説明] フィールドには、アプリケーションに関連する詳細があらかじめ入力されています。この情報は編集することができます。
9. 「IAM Identity Center」で、以下の作業を行います。

    a. IAM Identity Center SAML メタデータファイルの横にある [ダウンロード] を選択して、ID プロバイダーのメタデータをダウンロードします。

    b. [IAM Identity Center 証明書] の横にある [証明書のダウンロード] を選択して、ID プロバイダーの証明書をダウンロードします。

> **Note**
>
> 後で、サービスプロバイダーのウェブサイトからアプリケーションを設定するときに、これらのファイルが必要になります。そのプロバイダーからの手順に従います。

10. (オプション) [アプリケーションプロパティ] の下で、[アプリケーション開始 URL]、[リレー状態]、[セッション期間] を指定できます。詳細については、「IAM アイデンティティセンターコンソールのアプリケーションプロパティを設定する」を参照してください。
11. [Application metadata] (アプリケーションメタデータ) で、以下のいずれかを行います。
    a. メタデータファイルがある場合は、[アプリケーション SAML メタデータファイルをアップロードする] を選択します。次に、[ファイルを選択] を選択してメタデータファイルを検索して選択します。
    b. メタデータファイルがない場合は、[メタデータ値を手動で入力する] を選択して、[アプリケーション ACS URL] および [アプリケーション SAML 対象者] の値を指定します。
12. [送信] を選択します。追加したアプリケーションの詳細ページが表示されます。

独自の SAML 2.0 アプリケーションをセットアップする

SAML 2.0 を使用した ID フェデレーションを可能にする独自のアプリケーションを設定し、それらを IAM アイデンティティセンターに追加できます。独自の SAML 2.0 アプリケーションを設定する手順のほとんどは、IAM アイデンティティセンターコンソールのアプリケーションカタログから SAML 2.0 アプリケーションを設定するのと同じです。ただし、独自の SAML 2.0 アプリケーションのために、追加の SAML 属性マッピングを提供する必要があります。これらのマッピングは、IAM アイデンティティセンターがアプリケーションに対して SAML 2.0 アサーションを正しく追加できるようにします。アプリケーションを初めて設定するときに、この SAML 属性マッピングを追加できます。また、IAM アイデンティティセンターコンソールのアプリケーションの詳細ページでも、SAML 2.0 属性マッピングを追加できます。

以下の手順を使用して、IAM アイデンティティセンターと SAML 2.0 アプリケーションのサービスプロバイダーとの間で SAML 2.0 の信頼関係を設定します。この手順を開始する前に、信頼をより効率的に設定できるように、サービスプロバイダーの証明書とメタデータエクスチェンジファイルがあることを確認してください。

独自の SAML 2.0 アプリケーションを設定するには

1. IAM Identity Center コンソール を開きます。
2. [Applications] (アプリケーション) を選択します。
3. [カスタマーマネージド] タブを選択します。
4. [アプリケーションの追加] を選択します。
5. [アプリケーションタイプを選択] ページの [セットアッププリファレンス] で、[セットアップしたいアプリケーションがある] を選択します。
6. [アプリケーションタイプ] で、[SAML 2.0] を選択します。
7. [次へ] をクリックします。
8. [アプリケーションの設定] ページの [アプリケーションの設定] で、**MyApp** のようにアプリケーションの [表示名] を入力します。[Description] を入力します。
9. 「IAM Identity Center」で、以下の作業を行います。

   a. IAM Identity Center SAML メタデータファイルの横にある [ダウンロード] を選択して、ID プロバイダーのメタデータをダウンロードします。

   b. [IAM アイデンティティセンターの証明書] で、[ダウンロード] を選択して、ID プロバイダーの証明書をダウンロードします。

   > **Note**
   >
   > 後で、サービスプロバイダーのウェブサイトからカスタムアプリケーションを設定するときに、これらのファイルが必要になります。

10. (オプション) [アプリケーションプロパティ] の下で、[アプリケーション開始 URL]、[リレー状態]、[セッション期間] も指定できます。詳細については、「IAM アイデンティティセンターコンソールのアプリケーションプロパティを設定する」を参照してください。
11. [アプリケーションメタデータ] で [メタデータの値を手動で入力] を選択します。次に、[アプリケーション ACS URL] および [アプリケーション SAML 対象者] の値を指定します。
12. [送信] を選択します。追加したアプリケーションの詳細ページが表示されます。

アプリケーション間での信頼されたアイデンティティのプロパゲーション

信頼できる ID の伝播により、 AWS サービスは次のことを実行できます。

- ユーザーの ID コンテキストに基づいて AWS リソースへのアクセスを許可します。
- ユーザーの ID コンテキストを他の AWS サービスと安全に共有します。

これらの機能により、ユーザーアクセスをより簡単に定義、付与、記録できます。

信頼できる ID の伝播を使用すると、ユーザーはアプリケーションにサインインでき、そのアプリケーションは AWS サービスのデータにアクセスするためのリクエストでユーザーの ID コンテキストを渡すことができます。アクセスはユーザーの ID に基づいて管理されるため、ユーザーはデータにアクセスするためにデータベースのローカルユーザー認証情報を使用したり、IAM ロールを引き受けたりする必要はありません。

トピック

信頼できる ID の伝播の概要

信頼できる ID の伝播により、 AWS リソースへのユーザーアクセスをより簡単に定義、付与、記録できます。信頼できる ID の伝播は OAuth 2.0 認証フレームワークに構築されているため、アプリケーションはパスワードを共有しなくてもユーザーデータに安全にアクセスして共有できます。OAuth 2.0 は、アプリケーションリソースへの安全な委任アクセスを提供します。リソース管理者が、ユーザーがサインインしているアプリケーションに、他のアプリケーションへのアクセスを承認または委任するため、アクセスが委任されます。

ユーザーパスワードを共有しないようにするため、信頼できる ID の伝播ではトークンを使用します。トークンは、信頼されたアプリケーションがユーザーと 2 つのアプリケーション間で許可されるリクエストをクレームするための標準的な方法を提供します。信頼された ID 伝達と統合される AWS マネージドアプリケーションは、IAM Identity Center から直接トークンを取得します。IAM アイデンティティセンターには、外部の OAuth 2.0 認証サーバーからの ID トークンとアクセストーク

ンをアプリケーションが交換するオプションも用意されています。これにより、アプリケーションはの外部でトークンを認証して取得し AWS、トークンを IAM Identity Center トークンと交換し、新しいトークンを使用して AWS サービスにリクエストを行うことができます。詳細については、「信頼できるトークン発行者によるアプリケーションの使用」を参照してください。

OAuth 2.0 プロセスは、ユーザーがアプリケーションにサインインすると開始されます。ユーザーがサインインするアプリケーションは、他のアプリケーションのリソースへのアクセスリクエストを開始します。開始 (リクエスト) アプリケーションは、承認サーバーにトークンをリクエストすることで、ユーザーに代わって受信側のアプリケーションにアクセスできます。認証サーバーはトークンを返し、開始側アプリケーションはそのトークンをアクセスするリクエストとともに受信側アプリケーションに渡します。

信頼できる ID の伝播のユースケース

IAM Identity Center の管理者は、この機能をサポートする以下の開始アプリケーションと接続された AWS サービスとの間で、信頼できる ID 伝達を設定するよう求められる場合があります。以下のセクションでは、信頼できる ID の伝播を開始できるアプリケーションでサポートされている特定のユースケースについて詳しく説明します。

トピック

- Amazon EMR
- Amazon QuickSight
- Amazon Redshift クエリエディタ v2
- サードパーティーのビジネスインテリジェンスアプリケーション
- カスタム開発アプリケーション

Amazon EMR

Amazon EMR は、次の信頼できる ID 伝達のユースケースの開始アプリケーションとして使用できます。

説明	使用されているその他の AWS サービス	詳細はこちら
Amazon EMR Studio を介して Amazon EC2 クラスターの Amazon EMR で Apache Spark	、Amazon S3 Access Grants AWS Lake Formation、Amazon	• 「Amazon EMR 管理ガイド」の「Amazon EMR を IAM Identity Center と統合する」。

説明	使用されているその他の AWS サービス	詳細はこちら
を使用してインタラクティブ分析を実行します。を通じて AWS Glue Catalog のワークフォース ID および関連する属性に基づいてアクセスコントロールを適用します AWS Lake Formation。	S3、 を通じて承認された Amazon EC2 Amazon S3 EMR Amazon S3 AWS Service Catalog **Note** • Amazon EMR Studio からのアクセスが必要です。 • テーブルレベルのアクセスコントロールのみ。 • Apache Hive、PrestoSQL / Trino、および EMR Serverless はサポートされていません。	• Amazon S3 Access Grants」と「社内ディレクトリ ID」。 • デAWS Lake Formation ベロッパーガイドの「IAM Identity Center AWS Lake Formation との接続」 • AWS ビッグデータブログの「Amazon EMR と IAM Identity Center で分析に企業 ID を使用する」

説明	使用されているその他の AWS サービス	詳細はこちら
Amazon EMR Studio を介して Athena で Trino を使用してアドホック分析を実行します。を通じて AWS Glue Catalog のワークフォース ID および関連する属性に基づいてアクセスコントロールを適用します AWS Lake Formation。Amazon S3 Access Grants を使用してAmazon S3クエリ結果バケットの場所へのアクセスを保護します。	AWS Lake Formation 、Amazon S3 Access Grants を通じて承認された Athena Note Amazon EMR Studio からのアクセスが必要です。 Amazon Athena コンソールからの直接アクセスはサポートされていません。	• 「Amazon EMR 管理ガイド」の「Amazon EMR を IAM Identity Center と統合する」。 • 「Amazon Athena ユーザーガイド」の「IAM Identity Center 対応 Athena ワークグループの使用」。 Amazon Athena • Amazon S3 Access Grants」と「社内ディレクトリ ID」。 • 「 デベロッパーガイド」の「IAM Identity Center AWS Lake Formation との接続」。 AWS Lake Formation • ビッグデータブログ の「Amazon EMR Studio と Athena にワークフォースアイデンティティを持ち込む」。 AWS

Amazon QuickSight

Amazon は、次の信頼できる ID 伝達のユースケースの開始アプリケーション QuickSight として使用できます。

説明	使用されているその他の AWS サービス	詳細はこちら
Amazon QuickSight ユーザーは Amazon Redshift データをクエリできます。データアクセスは、Amazon Redshift 管理者に	Amazon Redshift	• Redshift を IAM Identity Center に接続して、「Amazon Redshift 管理ガイド」の「シングルサインオンエクスペリエ

説明	使用されているその他の AWS サービス	詳細はこちら
よって Amazon Redshift で許可されます。		ンス」をユーザーに付与します。 • 「Amazon Redshift 管理ガイド」の「Amazon 経由で Amazon Redshift を IAM Identity Center に接続します QuickSight」。
Amazon QuickSight ユーザーは Amazon Redshift Spectrum に Amazon S3 の構造化データをクエリし、管理者によって承認されたアクセスを許可 AWS Lake Formation できます。	Amazon Redshift Spectrum、Amazon S3 構造化データ * で承認された Amazon Redshift Spectrum 経由 AWS Lake Formation	• Redshift を IAM Identity Center に接続して、「Amazon Redshift 管理ガイド」の「シングルサインオンエクスペリエンス」をユーザーに付与します。 • 「Amazon Redshift 管理ガイド」の「Amazon 経由で Amazon Redshift を IAM Identity Center に接続します QuickSight」。 • 「 デベロッパーガイド」の「IAM Identity Center AWS Lake Formation との接続」。 AWS Lake Formation • ビッグデータブログの「Amazon Redshift と AWS Lake Formation 外部 ID プロバイダーのユーザー向けのアクセス管理を簡素化する」。 AWS

説明	使用されているその他の AWS サービス	詳細はこちら
Amazon QuickSight ユーザーは、Amazon Redshift データ共有に Amazon S3 内の構造化データをクエリし、管理者によって承認されたアクセスを許可 AWS Lake Formation できます。	Amazon Redshift データ共有、Amazon S3 構造化データ * を通じて承認された Amazon Redshift 経由 AWS Lake Formation	• 「Amazon Redshift 管理ガイド」の「Amazon 経由で Amazon Redshift を IAM Identity Center に接続します QuickSight」。 • 「 デベロッパーガイド」の「IAM Identity Center AWS Lake Formation との接続」。 AWS Lake Formation • ビッグデータブログの「Amazon Redshift と AWS Lake Formation 外部 ID プロバイダーのユーザー向けのアクセス管理を簡素化する」。 AWS

Amazon Redshift クエリエディタ v2

Amazon Redshift クエリエディタ v2 は、次の信頼できる ID 伝達のユースケースの開始アプリケーションとして使用できます。

説明	使用されているその他の AWS サービス	詳細はこちら
Amazon Redshift クエリエディタ v2 のユーザーは、Amazon Redshift データをクエリできます。データアクセスは、Amazon Redshift 管理者によって Amazon Redshift で許可されます。	Amazon Redshift	• Redshift を IAM Identity Center に接続して、「Amazon Redshift 管理ガイド」の「シングルサインオンエクスペリエンス」をユーザーに付与します。 • 「Amazon Redshift 管理ガイド」の「Amazon Redshift データベースに接続します」。

説明	使用されているその他の AWS サービス	詳細はこちら
		• AWS ビッグデータブログの「シームレスなシングルサインオン AWS IAM Identity Center 」のために を使用して Amazon Redshift クエリエディタ V2 Oktaと統合します。
Amazon Redshift クエリエディタ v2 のユーザーは、Amazon Redshift Spectrum の外部テーブルに Amazon S3 内の構造化データをクエリし、 AWS Lake Formation 管理者によって承認されたアクセスを許可できます。	Amazon Redshift Spectrum、Amazon S3 構造化データ * で承認された Amazon Redshift Spectrum 経由 AWS Lake Formation	• Redshift を IAM Identity Center に接続して、「Amazon Redshift 管理ガイド」の「シングルサインオンエクスペリエンス」をユーザーに付与します。 • 「Amazon Redshift 管理ガイド」の「Amazon Redshift データベースに接続します」。 • 「 デベロッパーガイド」の「IAM Identity Center AWS Lake Formation との接続」。 AWS Lake Formation
Amazon Redshift クエリエディタ v2 のユーザーは、管理者によって承認されたアクセスを使用して Amazon Redshift データ共有を AWS Lake Formation クエリできます。	Amazon Redshift データ共有、 AWS Lake Formation	• 「Amazon Redshift 管理ガイド」の「Amazon Redshift データベースに接続します」。 • 「 デベロッパーガイド」の「IAM Identity Center AWS Lake Formation との接続」。 AWS Lake Formation

サードパーティーのビジネスインテリジェンスアプリケーション

Tableau などのサードパーティーのビジネスインテリジェンスアプリケーションを、特定の信頼できる ID 伝達ユースケースの開始アプリケーションとして使用できます。変更されたサードパーティー

のビジネスインテリジェンスアプリケーションは、OAuth ID トークンまたはアクセストークンを介して Amazon Redshift ドライバーにユーザーの ID を渡し、Amazon Redshift 管理者によって承認されたアクセスで Amazon Redshift にデータをクエリできます。

カスタム開発アプリケーション

独自のカスタム開発アプリケーションは、次の信頼できる ID 伝達ユースケースの開始アプリケーションとして使用できます。

説明	使用されているその他の AWS サービス	詳細はこちら
OAuth 認証サーバーを介してユーザーを認証するアプリケーションを作成し、 AWS IAM Identity Center と IAM を使用してアイデンティティが強化された IAM ロールの認証情報を取得します。この認証情報は、Amazon S3 Access Grants 管理者によって承認されたアクセスを持つ Amazon S3 の非構造化データへのアクセスをリクエストするために使用されます。	AWS IAM Identity Center、Amazon S3 の非構造化データ *Amazon S3 Access Grants を通じて承認	• Amazon S3 Access Grants」と「社内ディレクトリ ID」。 • Storage Blog の「IAM Identity Center と Amazon S3 Access Grants (パート 1) と (パート 2) を使用してユーザー向けデータアプリケーションを開発する方法」。 https://aws.amazon.com/blogs/storage/how-to-develop-a-user-facing-data-application-with-iam-identity-center-and-s3-access-grants-part-2/ AWS
Amazon Q Business とやり取りするカスタムアプリケーションを構築して、独自のコンテンツとユーザーのアクセス許可に基づいてユーザーの質問に答えます。	IAM Identity Center、Amazon Q Business	• 「Amazon Q Business ユーザーガイド」の「IAM Identity Center インスタンスを有効にして設定する」。 • IAM Identity Center で AWS マネージドアプリケーションを使用する方法: セキュリティブログの「既存の IAM フェデレーションフローを移行せずに Amazon Q を有効にします」。 AWS

信頼できる ID の伝播を設定する

信頼できる ID の伝播は、アプリケーションが認証してユーザーの ID を AWS サービスに渡すことができるようにするさまざまな方法をサポートしています。信頼できる ID 伝播の設定は、アプリケーションの種類と認証方法に基づいて異なります。

> **Note**
>
> マネージドアプリケーションへのアクセスをリクエストするが、 AWS APIs を使用して接続しないカスタマー AWS マネージドアプリケーションがある場合は、信頼できるトークン発行者を設定する必要があります。

トピック

前提条件と考慮事項

信頼できる ID の伝播を設定する前に、以下の前提条件と考慮事項を確認してください。

トピック

前提条件

信頼できる ID の伝播を使用するには、環境が以下の前提条件を満たしていることを確認してください。

- ユーザーとグループがプロビジョニングされた IAM アイデンティティセンターのデプロイ

  信頼できる ID の伝播を使用するには、IAM アイデンティティセンターを有効にし、ユーザーおよびグループをプロビジョニングする必要があります。詳細については、「IAM アイデンティティセンターで一般的なタスクを開始する」を参照してください。

組織インスタンスの推奨 — Organizations の管理アカウントで有効にした IAM Identity Center の AWS 組織インスタンスを使用することをお勧めします。信頼できる ID 伝達を使用して、ユーザーが同じ組織 AWS アカウント 内の異なる のサービスおよび関連リソースにアクセス AWS できるようにする場合は、IAM Identity Center のインスタンスの管理をメンバーアカウントに委任できます。

IAM Identity Center の単一アカウントインスタンスを使用する場合、信頼できる ID の伝播を通じてユーザーにアクセス権を付与するすべての AWSサービスとリソースは AWS アカウント、同じスタンドアロン 、または IAM Identity Center を有効にした組織内の同じメンバーアカウントに存在する必要があります。詳細については、「IAM アイデンティティセンターのアカウントインスタンス」を参照してください。

- AWS マネージドアプリケーションの場合、IAM Identity Center への接続

  信頼できる ID 伝達を使用するには、 AWS マネージドアプリケーションが IAM Identity Center と統合されている必要があります。

追加の考慮事項

信頼できる ID の伝播を使用するときは、次の考慮事項に留意してください。

- AWS マネージドアプリケーションの必須割り当て設定を変更しない

  AWS マネージドアプリケーションには、ユーザーとグループに割り当てが必要かどうかを決定するデフォルト設定があります。この設定は変更しないことをお勧めします。特定のリソースへのユーザーアクセスを許可するきめ細かい権限を設定した場合でも、[割り当ては必須です] 設定を変更すると、これらのリソースへのユーザーアクセスが中断されるなど、予期しない動作が発生する可能性があります。
- マルチアカウント許可 (アクセス許可セット) は不要です

  信頼できる ID の伝播では、マルチアカウント許可 (アクセス許可セット) を設定する必要はありません。IAM アイデンティティセンターを有効にして、信頼できる ID の伝播にのみ使用できます。

AWS マネージドアプリケーションでの信頼できる ID の伝播の使用

信頼できる ID の伝播により、 AWS マネージドアプリケーションはユーザーに代わって AWS のサービス内のデータへのアクセスをリクエストできます。データアクセス管理はユーザーの ID に基づいているため、管理者はユーザーの既存のユーザーやグループのメンバーシップに基づいてアクセ

スを付与できます。ユーザーの ID、ユーザーに代わって実行されたアクション、およびその他のイベントは、サービス固有のログと CloudTrailイベントに記録されます。

信頼できる ID の伝播は OAuth 2.0 標準に基づいています。この機能を使用するには、 AWS マネージドアプリケーションが IAM Identity Center と統合されている必要があります。 AWS 分析サービスは、互換性のあるアプリケーションが信頼できる ID 伝達を使用できるようにするドライバーベースのインターフェイスを提供する場合があります。例えば、JDBC、ODBC、および Python ドライバーを使用すると、互換性のあるクエリツールで追加のセットアップ手順を実行しなくても、信頼できる ID の伝播を使用できます。

トピック

- 信頼できる ID の伝播のための AWS マネージドアプリケーションのセットアップ
- AWS マネージドアプリケーションの信頼できる ID 伝達リクエストフロー
- アプリケーションがトークンを取得した後
- ID が強化された IAM ロールセッション
- ID が強化された IAM ロールセッションのタイプ
- AWS マネージドアプリケーションのセットアッププロセスとリクエストフロー

信頼できる ID の伝播のための AWS マネージドアプリケーションのセットアップ

AWS 信頼できる ID の伝播をサポートする のサービスは、この機能の設定に使用できる管理ユーザーインターフェイスと APIs を提供します。これらのサービスに対して、IAM アイデンティティセンター内で設定を行う必要はありません。

以下は、信頼できる ID の伝播用に AWS サービスを設定する大まかなプロセスです。具体的な手順は、アプリケーションが提供する管理インターフェースと API に応じて異なります。

1. アプリケーションコンソールまたは API を使用して、アプリケーションを IAM アイデンティティセンターのインスタンスに接続する

   AWS マネージドアプリケーションまたはアプリケーション APIs のコンソールを使用して、アプリケーションを IAM Identity Center のインスタンスに接続します。アプリケーションのコンソールを使用する場合、管理ユーザーインターフェースにはセットアップと接続プロセスを効率化するウィジェットが含まれます。
2. アプリケーションコンソールまたは API を使用して、アプリケーションのリソースへのユーザーアクセスを設定する

このステップを完了して、ユーザーがアクセスできるリソースまたはデータを承認します。アクセスは、ユーザーの ID またはグループメンバーシップに基づいています。認証モデルは、アプリケーションによって異なります。

> **Important**
>
> ユーザーが AWS サービスのリソースにアクセスできるようにするには、このステップを完了する必要があります。そうしないと、リクエスト元のアプリケーションがサービスへのアクセスをリクエストする権限を与えられていても、ユーザーはリソースにアクセスできません。

AWS マネージドアプリケーションの信頼できる ID 伝達リクエストフロー

AWS マネージドアプリケーションへの信頼できる ID の伝播フローはすべて、IAM Identity Center からトークンを取得するアプリケーションから開始する必要があります。このトークンが必要なのは、IAM アイデンティティセンターが認識しているユーザーや IAM アイデンティティセンターに登録されているアプリケーションへの参照が含まれているためです。

以下のセクションでは、 AWS マネージドアプリケーションが IAM Identity Center からトークンを取得して信頼できる ID の伝播を開始する方法について説明します。

トピック

- ウェブベースの、IAM アイデンティティセンター認証
- コンソールベースの、ユーザーが開始する認証リクエスト

ウェブベースの、IAM アイデンティティセンター認証

このフローでは、 AWS マネージドアプリケーションは認証に IAM Identity Center を使用するウェブベースのシングルサインオンエクスペリエンスを提供します。

ユーザーが AWS マネージドアプリケーションを開くと、IAM Identity Center を使用するシングルサインオンフローがトリガーされます。IAM アイデンティティセンターにユーザーのアクティブなセッションがない場合、指定していた ID ソースに基づくサインインページがユーザーに表示され、IAM アイデンティティセンターがユーザー用のセッションを作成します。

IAM Identity Center は、ユーザーの ID と、アプリケーションが使用するために登録されている対象者 (Auds) および関連するスコープのリストを含むトークンを AWS マネージドアプリケーションに

提供します。その後、アプリケーションはそのトークンを使用して、他の受信 AWS サービスにリクエストを送信できます。

コンソールベースの、ユーザーが開始する認証リクエスト

このフローでは、 AWS マネージドアプリケーションはユーザーが開始するコンソールエクスペリエンスを提供します。

この場合、 AWS マネージドアプリケーションはロールを引き AWS 受けた後に マネジメントコンソールから入力されます。アプリケーションがトークンを取得するには、ユーザーがアプリケーションをトリガーしてユーザーを認証するプロセスを開始する必要があります。これにより IAM アイデンティティセンターを使用して認証が開始され、設定した ID ソースにユーザーがリダイレクトされます。

アプリケーションがトークンを取得した後

リクエスト元のアプリケーションが IAM アイデンティティセンターからトークンを取得すると、アプリケーションは定期的にトークンを更新します。このトークンはユーザーのセッション間ずっと使用できます。この間、アプリケーションは次の場合があります。

- トークンに関する詳細情報を入手して、そのユーザーが誰なのか、そのアプリケーションが他の受信側の AWS マネージドアプリケーションでどのスコープが使用できるのかを判断します。
- トークンの使用をサポートする他の受信側の AWS マネージドアプリケーションへの呼び出しでトークンを渡します。
- 署名バージョン 4 を使用する AWS 他の AWS マネージドアプリケーションにリクエストを送信するために使用できる、アイデンティティが強化された IAM ロールセッションを取得します。

  ID が強化された IAM ロール セッションは、IAM アイデンティティセンターによって作成されたトークンに保存されたユーザーの伝播された ID を含む IAM ロールセッションです。

ID が強化された IAM ロールセッション

AWS Security Token Service を使用すると、アプリケーションはアイデンティティが強化された IAM ロールセッションを取得できます。ロールセッションのユーザーコンテキストをサポートする AWS マネージドアプリケーションは、アイデンティティ情報を使用して、ロールセッションに参加しているユーザーに基づいてアクセスを許可できます。この新しいコンテキストにより、アプリケーションは AWS 署名バージョン 4 API リクエストを通じて、信頼できる ID の伝播をサポートする AWS マネージドアプリケーションにリクエストを行うことができます。

AWS マネージドアプリケーションが ID が強化された IAM ロールセッションを使用してリソースにアクセスすると、 はユーザーの ID (user-ID)、開始セッション、および実行されたアクションを CloudTrail ログに記録します。

アプリケーションが ID が強化された IAM ロールセッションを使用して受信側のアプリケーションにリクエストを行うと、受信側のアプリケーションがユーザーの ID、グループメンバーシップ、または IAM ロールに基づいてアクセスを承認できるように、セッションにコンテキストが追加されます。信頼できる ID の伝播をサポートする受信側のアプリケーションは、受信側のアプリケーションまたはリクエストされたリソースが、ユーザーの ID またはグループメンバーシップに基づいてアクセスを承認するように設定されていない場合、エラーを返します。

この問題を回避するには、以下のいずれかの方法で対応します。

- 受信側のアプリケーションが IAM アイデンティティセンターに接続されていることを確認します。
- 受信側のアプリケーションのコンソールまたはアプリケーション API を使用して、ユーザーの ID またはグループメンバーシップに基づいてリソースへのアクセスを許可するようにアプリケーションを設定します。このための設定要件は、アプリケーションによって異なります。

詳細については、受信側の AWS マネージドアプリケーションのドキュメントを参照してください。

ID が強化された IAM ロールセッションのタイプ

アプリケーションは、 API に AWS STS `AssumeRole`リクエストを行い、リクエストの `ProvidedContexts`パラメータでコンテキストアサーションを渡すことで、アイデンティティが強化された IAM ロールセッションを取得します`AssumeRole`。コンテキストアサーションは、SSO OIDC `CreateTokenWithIAM` リクエストからのレスポンスに含まれる `idToken` クレームから取得されます。

AWS STS は、`AssumeRole`リクエストに提供されるコンテキストアサーションに応じて、2 つの異なるタイプのアイデンティティ拡張 IAM ロールセッションを作成できます。

- ユーザーの ID のみを に記録するセッション CloudTrail。
- 伝播されたユーザー ID に基づいて認証を有効にし、 に記録するセッション CloudTrail。

CloudTrail 証跡に登録されている監査情報 AWS STS のみを提供する からアイデンティティが強化された IAM ロールセッションを取得するには、`AssumeRole`リクエストに `sts:audit_context`クレームの値を指定します。受信側 AWS サービスが IAM Identity Center ユーザーにアク

ションを実行することを許可するセッションを取得するには、AssumeRoleリクエストに sts:identity_contextクレームの値を指定します。コンテキストは 1 つだけ入力できます。

sts:audit_context で作成された ID が強化された IAM ロールセッション

で作成された ID が強化された IAM ロールセッションを使用して AWS サービスにリクエストが行われるとsts:audit_context、ユーザーの IAM アイデンティティセンターuserIdは OnBehalfOf要素 CloudTrail で にログ記録されます。

```
"userIdentity": {
      "type": "AssumedRole",
      "principalId": "AROAEXAMPLE:MyRole",
      "arn": "arn:aws:sts::111111111111:assumed-role/MyRole/MySession",
      "accountId": "111111111111",
      "accessKeyId": "ASIAEXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "AROAEXAMPLE",
            "arn": "arn:aws:iam::111111111111:role/MyRole",
            "accountId": "111111111111",
            "userName": "MyRole"
        },
        "attributes": {
            "creationDate": "2023-12-12T13:55:22Z",
            "mfaAuthenticated": "false"
        }
    },
    "onBehalfOf": {
        "userId": "11111111-1111-1111-1111-1111111111",
        "identityStoreArn": "arn:aws:identitystore::111111111111:identitystore/
d-111111111"
    }
}
```

> **Note**
>
> これらのセッションは Identity Center ユーザーの認証には使用できません。それらは引き続き IAM ロールの認証に使用できます。

このタイプのロールセッションを から取得するには AWS STS、AssumeRoleリクエストProvidedContextsパラメータ のリクエストに sts:audit_contextフィールドの値を指定します。arn:aws:iam::aws:contextProvider/IdentityStore を ProviderArn の値として使用します。

sts:identity_context で作成された ID が強化された IAM ロールセッション

ユーザーが で作成されたアイデンティティ拡張 IAM ロールセッションを使用して AWS サービスにリクエストを行うとsts:identity_context、ユーザーの IAM アイデンティティセンターuserIdは、 CloudTrail で作成されたセッションと同じ方法で onBehalfOf要素にログ記録されますsts:audit_context。

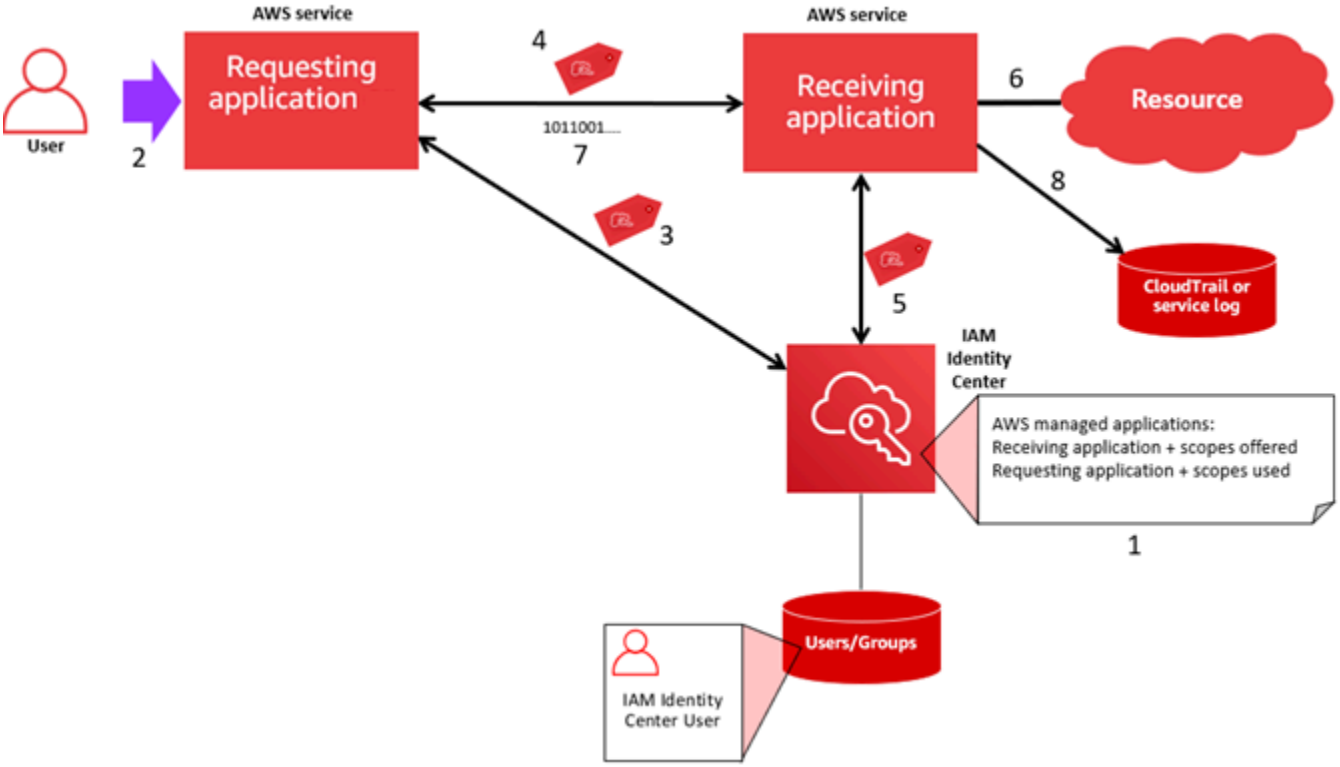
IAM Identity Center ユーザーの を userIdに記録することに加えて CloudTrail、このタイプのセッションは、サポートされている APIs でも使用され、伝播されたユーザー ID に基づいてアクションを承認します。サポートされているAPIsAWSIAMIdentityCenterAllowListForIdentityContext AWS 管理ポリシー」を参照してください。この AWS 管理ポリシーは、アイデンティティが強化された IAM ロールセッションがで作成されたときに、セッションポリシーとして提供されますsts:identity_context。このポリシーでは、サポートされていない AWS サービスでロールセッションを使用することはできません。

このタイプのロールセッションを から取得するには AWS STS、AssumeRoleリクエストProvidedContextsパラメータ のリクエストに sts:identity_contextフィールドの値を指定します。arn:aws:iam::aws:contextProvider/IdentityStore を ProviderArn の値として使用します。

AWS マネージドアプリケーションのセットアッププロセスとリクエストフロー

このセクションでは、信頼できる ID の伝播を使用し、Web ベースのシングルサインオン環境を提供する AWS マネージドアプリケーションのセットアッププロセスとリクエストフローについて説明します。

次の図は、このプロセスの概要を示しています。



次の手順で、このプロセスに関する追加情報を提供します。

1. AWS マネージドアプリケーションまたはアプリケーション APIs の コンソールを使用して、以下を実行します。

   a. アプリケーションを IAM アイデンティティセンターのインスタンスに接続します。

   b. ユーザーがアクセスできるアプリケーションリソースを許可するアクセス許可を設定します。

2. リクエストフローは、ユーザーが リソース (リクエスト元のアプリケーション) へのアクセスをリクエストできる AWS マネージドアプリケーションを開くと開始されます。

3. 受信側の AWS マネージドアプリケーションにアクセスするためのトークンを取得するには、リクエスト元の AWS マネージドアプリケーションが IAM Identity Center へのサインインリクエストを開始します。

   ユーザーがサインインしていない場合、IAM アイデンティティセンターは指定した ID ソースへのユーザー認証フローをトリガーします。これにより、IAM Identity Center で設定した期間を持つユーザーの新しい AWS アクセスポータルセッションが作成されます。その後、IAM Identity Center はセッションに関連付けられたトークンを生成し、アプリケーションはユーザーの AWS アクセスポータルセッションの残りの期間にわたって動作できます。ユーザーがアプリケーションからサインアウトしたり、セッションを削除したりすると、セッションは 2 時間以内に自動的に終了します。

4. AWS マネージドアプリケーションは、受信側アプリケーションへのリクエストを開始し、そのトークンを提供します。
5. 受信側のアプリケーションは IAM アイデンティティセンターを呼び出して、ユーザーの ID とトークンにエンコードされたスコープを取得します。受信側のアプリケーションが、Identity Center ディレクトリからユーザー属性またはユーザーのグループメンバーシップを取得するようにリクエストする場合もあります。
6. 受信側のアプリケーションは、その認証設定を使用して、リクエストされたアプリケーションリソースへのアクセスがユーザーに許可されているかどうかを判断します。
7. リクエストされたアプリケーションリソースへのアクセスがユーザーに許可されている場合、受信側のアプリケーションはそのリクエストに応答します。
8. ユーザーの ID、ユーザーに代わって実行されたアクション、受信側のアプリケーション ログと AWS CloudTrail イベントに記録されたその他のイベント。この情報を記録する具体的な方法は、アプリケーションによって異なります。

カスタマーマネージドアプリケーションによる信頼できる ID の伝播の使用

信頼できる ID の伝播により、カスタマーマネージドアプリケーションはユーザーに代わって AWS のサービス内のデータへのアクセスをリクエストできます。データアクセス管理はユーザーの ID に基づいているため、管理者はユーザーの既存のユーザーやグループのメンバーシップに基づいてアクセスを付与できます。ユーザーの ID、ユーザーに代わって実行されたアクション、およびその他のイベントは、サービス固有の口グと CloudTrailイベントに記録されます。

信頼できる ID の伝播を使用すると、ユーザーはカスタマーマネージドアプリケーションにサインインでき、そのアプリケーションは AWS サービスのデータにアクセスするためのリクエストでユーザーの ID を渡すことができます。

> **Important**
>
> AWS サービスにアクセスするには、カスタマーマネージドアプリケーションが IAM Identity Center の外部にある信頼できるトークン発行者からトークンを取得する必要があります。信頼できるトークン発行者とは、署名付きトークンを作成する OAuth 2.0 認証サーバーです。これらのトークンは、 AWS サービス (受信側アプリケーション) へのアクセスリクエストを開始するアプリケーションを承認します。詳細については、「信頼できるトークン発行者によるアプリケーションの使用」を参照してください。

トピック

- 信頼できる ID の伝播用のカスタマーマネージドの OAuth 2.0 アプリケーションを設定する
- 信頼されたアプリケーションを指定する

信頼できる ID の伝播用のカスタマーマネージドの OAuth 2.0 アプリケーションを設定する

カスタマーマネージドの OAuth 2.0 アプリケーションを信頼できる ID の伝播用に設定するには、まず IAM アイデンティティセンターに追加する必要があります。次の手順を使用して、IAM アイデンティティセンターにアプリケーションを追加します。

トピック

- ステップ 1: アプリケーションタイプを選択する
- ステップ 2: アプリケーションの詳細を指定する
- ステップ 3: 認証設定を指定する
- ステップ 4: アプリケーション認証情報を指定する
- ステップ 5: 確認して設定する

ステップ 1: アプリケーションタイプを選択する

1. IAM Identity Center コンソール を開きます。
2. [Applications] (アプリケーション) を選択します。
3. [カスタマーマネージド] タブを選択します。
4. [アプリケーションの追加] を選択します。
5. [アプリケーションタイプを選択] ページの [セットアッププリファレンス] で、[セットアップしたいアプリケーションがある] を選択します。
6. [アプリケーションタイプ] で [OAuth 2.0] を選択します。
7. [次へ] を選択して次のページ、ステップ 2: アプリケーションの詳細を指定する に進みます。

ステップ 2: アプリケーションの詳細を指定する

1. [アプリケーションの詳細を指定] ページの [アプリケーションの名前と説明] で、**MyApp** のようなアプリケーションの [表示名] を入力します。[Description] を入力します。
2. [ユーザーとグループの割り当て方法] で、次のいずれかのオプションを選択します。

    - [割り当ては必須です] — このアプリケーションに割り当てられている IAM アイデンティティセンターユーザーとグループのみにアプリケーションへのアクセスを許可します。

アプリケーションタイルの可視性 – AWS アクセスポータルのアプリケーション可視性が表示可能 に設定されている場合は、アプリケーションに直接割り当てられたユーザー、またはグループ割り当てによって割り当てられたユーザーのみが AWS 、 アクセスポータルのアプリケーションタイルを表示できます。

- [割り当ては不要です] — 権限のあるすべての IAM アイデンティティセンターユーザーとグループにこのアプリケーションへのアクセスを許可します。

  アプリケーションタイルの表示 — [AWS アクセスポータルのアプリケーションの表示] が [非表示] に設定されていない限り、アプリケーションタイルは AWS アクセスポータルにサインインするすべてのユーザーに表示されます。

3. 「AWS アクセスポータル」で、ユーザーがアプリケーションにアクセスできる URL を入力し、アプリケーションタイルを AWS アクセスポータルに表示するか非表示にするかを指定します。[非表示] を選択すると、割り当てられたユーザーでもアプリケーションタイルを表示できなくなります。
4. [タグ (オプション)] で、[新しいタグを追加] を選択し、[キー] と [値 (オプション)] の値を指定します。

   タグの詳細については、「AWS IAM Identity Center リソースのタグ付け」を参照してください。
5. [次へ] を選択し、次のページ、ステップ 3: 認証設定を指定する に進みます。

ステップ 3: 認証設定を指定する

OAuth 2.0 をサポートするカスタマーマネージドアプリケーションを IAM アイデンティティセンターに追加するには、信頼できるトークン発行者を指定する必要があります。信頼できるトークン発行者とは、署名付きトークンを作成する OAuth 2.0 認証サーバーです。これらのトークンは、 AWS マネージドアプリケーション (受信側アプリケーション) へのアクセスリクエストを開始するアプリケーション (受信側アプリケーション) を承認します。

1. [認証設定を指定する] ページの、[信頼できるトークン発行者] で、次のいずれかを実行します。

   - 既存の信頼できるトークン発行者を使用するには:

     使用する信頼できるトークン発行者の名前の横にあるチェックボックスを選択します。
   - 新しい信頼できるトークン発行者を追加するには:

     1. [信頼できるトークン発行者を作成] を選択します。

2. 新しいブラウザタブが開きます。IAM アイデンティティセンターコンソールに信頼できるトークン発行者を追加する方法 のステップ 5～8 を実行します。
3. これらの手順を完了したら、アプリケーション設定に使用しているブラウザウィンドウに戻り、追加した信頼できるトークン発行者を選択します。
4. 信頼できるトークン発行者の一覧で、さきほど追加した信頼できるトークン発行者の名前の横にあるチェックボックスをオンにします。

   信頼できるトークン発行者を選択すると、[選択したトラステッドトークン発行者の設定] セクションが表示されます。

2. [選択したトラステッドトークン発行者の設定] で、[Aud クレーム] を入力します。[Aud クレーム] は、信頼できるトークン発行者が生成したトークンの対象者 (受信者) を識別します。詳細については、「Aud クレーム」を参照してください。
3. ユーザーがこのアプリケーションを使用しているときに再認証を必要としないようにするには、[アクティブなアプリケーションセッションのユーザー認証を自動的に更新する] を選択します。このオプションを選択すると、セッションの有効期限が切れるか、ユーザーがセッションを終了するまで、60 分ごとにセッションのアクセストークンが更新されます。
4. [次へ] を選択し、次のページ、ステップ 4: アプリケーション認証情報を指定する に進みます。

ステップ 4: アプリケーション認証情報を指定する

この手順のステップを完了して、アプリケーションが信頼できるアプリケーションとのトークン交換アクションを実行するときに使用する認証情報を指定します。これらの認証情報は、リソースベースのポリシーで使用されます。このポリシーでは、ポリシーで指定されているアクションを実行するアクセス許可持つプリンシパルを指定する必要があります。信頼できるアプリケーションが同じ AWS アカウントにあっても、プリンシパルを指定する必要があります。

> **Note**
>
> ポリシーでアクセス許可を設定するときは、タスクの実行に必要なアクセス許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権権限とも呼ばれています。

このポリシーには `sso-oauth:CreateTokenWithIAM` アクションが必要です。

1. [アプリケーション認証情報を指定] ページで、次のいずれかを実行します。

- 1 つ以上の IAM ロールをすばやく指定するには:
  1. [1 つ以上の IAM ロールを入力する] を選択します。
  2. [IAM ロールを入力] で、既存の IAM ロールの Amazon リソースネーム (ARN) を指定します。ARN を指定するには、次の構文を使用します。IAM リソースはグローバルに識別されるため、ARN のリージョンの割り当ては空白です。

     ```
     arn:aws:iam::account:role/role-name-with-path
     ```

     詳細については、「AWS Identity and Access Management ユーザーガイド」の「リソースベースのポリシーを使用したクロスアカウントアクセス」および「IAM ARN」を参照してください。
- ポリシーを手動で編集するには (AWS 非認証情報を指定する場合は必須) 。
  1. [アプリケーションポリシーを編集] を選択します。
  2. JSON テキストボックスにテキストを入力または貼り付けてポリシーを変更します。
  3. ポリシーの検証中に生成されたセキュリティ警告、エラー、または一般的な警告を解決します。詳細については、「AWS Identity and Access Management ユーザーガイド」の「IAM ポリシーの検証」を参照してください。

2. [次へ] を選択して次のページ、ステップ 5: 確認して設定する に進みます。

ステップ 5: 確認して設定する

1. [確認して設定] ページで、選択した内容を確認します。変更を加えるには、必要な構成セクションを選択し、[編集] を選択して必要なだけ変更を加えます。
2. 完了したら、[アプリケーションを追加] を選択します。
3. 追加したアプリケーションが [カスタマーマネージドアプリケーション] リストに表示されます。
4. IAM Identity Center でカスタマーマネージドアプリケーションを設定したら、ID の伝播のために 1 つ以上の AWS サービスまたは信頼できるアプリケーションを指定する必要があります。これにより、ユーザーはカスタマーマネージドアプリケーションにサインインして、信頼できるアプリケーションのデータにアクセスできるようになります。

   詳細については、「信頼されたアプリケーションを指定する 」を参照してください。

信頼されたアプリケーションを指定する

カスタマーマネージドアプリケーション を設定したら、ID の伝播のために 1 つ以上の信頼できる AWS サービスまたは信頼できるアプリケーションを指定する必要があります。カスタマーマネージドアプリケーションのユーザーがアクセスする必要があるデータを含む AWS サービスを指定します。ユーザーがカスタマーマネージドアプリケーションにサインインすると、そのアプリケーションはユーザーの ID を信頼できるアプリケーションに渡します。

以下の手順を使用して、サービスを選択し、そのサービスで信頼する個々のアプリケーションを指定します。

1. IAM Identity Center コンソール を開きます。
2. [Applications] (アプリケーション) を選択します。
3. [カスタマーマネージド] タブを選択します。
4. [カスタマーマネージドアプリケーション] リストで、アクセスのリクエストを開始する OAuth 2.0 アプリケーションを選択します。これはユーザーがサインインするアプリケーションです。
5. [詳細ページ] の [ID の伝播のための信頼されたアプリケーション] で、[信頼されたアプリケーションを指定] を選択します。
6. [セットアップタイプ] で、[個々のアプリケーションとアクセスの指定] を選択して、[次へ] を選択します。
7. [サービスを選択] ページで、カスタマーマネージドアプリケーションが ID の伝播に関して信頼できるアプリケーションを含む AWS サービスを選択し、[次へ] を選択します。

   選択するサービスによって、信頼できるアプリケーションが定義されます。次のステップでは、アプリケーションを選択できます。
8. [アプリケーションを選択] ページで、[個々のアプリケーション] を選択し、アクセスのリクエストを受信できる各アプリケーションのチェックボックスを選択して、[次へ] を選択します。
9. [アクセスの設定] ページの [設定方法] で、次のいずれかを実行します。

   - [アプリケーションごとにアクセスを選択] — このオプションを選択すると、アプリケーションごとに異なるアクセスレベルを設定できます。アクセスレベルを設定するアプリケーションを選択し、[アクセスを編集] を選択します。[適用するアクセスのレベル] で、必要に応じてアクセスレベルを変更し、[変更の保存] を選択します。
   - [すべてのアプリケーションに同じアクセスレベルを適用する] — アプリケーションごとにアクセスレベルを設定する必要がない場合は、このオプションを選択します。
10. [次へ] をクリックします。

11. [設定を確認] ページで、選択した内容を確認します。変更を加えるには、必要な設定セクションを選択し、[アクセスを編集] を選択して、必要なだけ変更を加えます。
12. 完了したら、[信頼アプリケーション] を選択します。

信頼できるトークン発行者によるアプリケーションの使用

信頼できるトークン発行者は、 の外部で認証するアプリケーションで信頼できる ID 伝達を使用できます AWS。信頼できるトークン発行者があれば、これらのアプリケーションに、ユーザーに代わって AWS マネージドアプリケーションへのアクセスをリクエストすることを許可できます。

以下のトピックでは、信頼できるトークン発行者の仕組みを説明し、設定ガイダンスを提供します。

トピック

信頼できるトークン発行者の概要

信頼できる ID の伝播は、 の外部で認証するアプリケーションが AWS 、信頼できるトークン発行者を使用してユーザーに代わってリクエストを実行できるようにするメカニズムを提供します。信頼できるトークン発行者とは、署名付きトークンを作成する OAuth 2.0 認証サーバーです。これらのトークンは、 AWS サービス (受信側アプリケーション) へのアクセスリクエスト (受信側アプリケーション) を開始するアプリケーションを承認します。リクエスト元アプリケーションは、信頼できるトークン発行者が認証するユーザーに代わってアクセス要求を開始します。ユーザーは、信頼できるトークン発行者と IAM アイデンティティセンターの両方に認識されています。

AWS リクエストを受信する サービスは、Identity Center ディレクトリで表されるユーザーとグループのメンバーシップに基づいて、リソースに対するきめ細かな承認を管理します。 AWS services は、外部トークン発行者からのトークンを直接使用することはできません。

この問題を解決するために、IAM アイデンティティセンターでは、リクエスト元アプリケーション、またはリクエスト元アプリケーションが使用する AWS ドライバーが、信頼できるトークン発行者が発行したトークンを IAM アイデンティティセンターが生成したトークンと交換する方法を提供

しています。IAM アイデンティティセンターによって生成されるトークンは、対応する IAM アイデンティティセンターのユーザーを指します。リクエスト元のアプリケーションまたはドライバーは、新しいトークンを使用して受信側のアプリケーションへのリクエストを開始します。新しいトークンは IAM アイデンティティセンター内の対応するユーザーを参照するため、受信側アプリケーションは IAM アイデンティティセンターに表示されているユーザーまたはグループメンバーシップに基づいて、リクエストされたアクセスを承認できます。

> **Important**
>
> OAuth 2.0 認証サーバーを信頼できるトークン発行者として追加するかどうかは、慎重に検討する必要があるセキュリティ上の決定です。以下のタスクを実行するには、信頼できるトークン発行者のみを選択してください。
>
> - トークンに指定されているユーザーを認証します。
> - そのユーザーによる受信側のアプリケーションへのアクセスを許可します。
> - IAM アイデンティティセンターが IAM アイデンティティセンターが作成したトークンと交換できるトークンを生成します。

信頼できるトークン発行者の前提条件と考慮事項

信頼できるトークン発行者を設定する前に、次の前提条件と考慮事項を確認します。

- 信頼できるトークン発行者の設定

  OAuth 2.0 認証サーバー (信頼できるトークン発行者) を設定する必要があります。信頼できるトークン発行者は、通常、IAM Identity Center の ID ソースとして使用する ID プロバイダーですが、そうである必要はありません。信頼できるトークン発行者を設定する方法については、関連する ID プロバイダーのドキュメントを参照してください。

  > **Note**
  >
  > 信頼できるトークン発行者の各ユーザーの ID を IAM アイデンティティセンターの対応するユーザーにマップさえすれば、最大 10 の信頼できるトークン発行者を IAM アイデンティティセンターで使用するように設定できます。

- トークンを作成する OAuth 2.0 認証サーバー (信頼できるトークン発行者) には、IAM アイデンティティセンターがトークンの署名を検証するためのパブリックキーを取得するのに使用できる

OpenID Connect (OIDC) ディスカバリエンドポイントが必要です。詳細については、「OIDC 検出エンドポイント URL (発行者 URL)」を参照してください。

- 信頼できるトークン発行者が発行したトークン

  信頼できるトークン発行者からのトークンは、次の要件を満たしている必要があります。

  - トークンは署名され、RS256 アルゴリズムを使用して JSON ウェブトークン (JWT) 形式で作成する必要があります。
  - トークンには、次のクレームが含まれている必要があります。
    - 発行者 (iss) – トークンを発行したエンティティ。この値は、信頼できるトークン発行者の OIDC 検出エンドポイント (発行者 URL) で設定された値と一致する必要があります。
    - 件名 (サブ) – 認証されたユーザー。
    - 対象者 (音声) — トークンの受取人。これは、トークンが IAM Identity Center からトークンと交換された後にアクセスされる AWS サービスです。詳細については、「Aud クレーム」を参照してください。
    - 有効期限 (exp) — トークンの有効期限が切れるまでの時間。
    -
  - トークンは、ID トークンでもアクセストークンでもかまいません。
  - トークンには、1 人の IAM アイデンティティセンターユーザーに一意にマッピングできる属性が必要です。
- オプションのクレーム

  IAM アイデンティティセンターは RFC 7523 で定義されているすべてのオプションのクレームをサポートしています。詳細については、この RFC の「セクション 3: JWT 形式と処理要件」を参照してください。

  例えば、トークンには JTI (JWT ID) クレーム を含めることができます。このクレームが存在する場合は、同じ JTI を持つトークンがトークンの交換に再利用されるのを防ぐことができます。JTI クレームの詳細については、「JTI クレームの詳細」を参照してください。
- 信頼できるトークン発行者と連携するための IAM アイデンティティセンターの設定

  また、IAM アイデンティティセンターを有効にし、IAM アイデンティティセンターの ID ソースを設定し、信頼できるトークン発行者のディレクトリ内のユーザーに対応するユーザーをプロビジョニングする必要があります。

  これを行うには、次のいずれかを実行する必要があります。

- クロスドメイン ID 管理システム (SCIM) 2.0 プロトコルを使用して、ユーザーを IAM アイデンティティセンターと同期します。
- IAM アイデンティティセンターでユーザーを直接作成します。

> **Note**
>
> Active Directory ドメイン サービスを ID ソースとして使用する場合、信頼できるトークン発行者はサポートされません。

JTI クレームの詳細

IAM アイデンティティセンターが既に交換したトークンを交換するリクエストを IAM アイデンティティセンターが受け取った場合、そのリクエストは失敗します。トークン交換のためのトークンの再利用を検出して防止するために、JTI クレームを含めることができます。IAM アイデンティティセンターは、トークン内のクレームに基づいてトークンの再利用を防止します。

すべての OAuth 2.0 認証サーバーがトークンに JTI クレームを追加するわけではありません。OAuth 2.0 認証サーバーの中には、JTI をカスタムクレームとして追加できないものもあります。JTI クレームの使用をサポートする OAuth 2.0 認証サーバーは、このクレームを ID トークンのみ、アクセストークンのみ、またはその両方に追加する場合があります。詳細については、OAuth 2.0 認証サーバーのドキュメントを参照してください。

トークンを交換するアプリケーションの構築については、IAM アイデンティティセンターAPI ドキュメントを参照してください。正しいトークンを取得して交換するようにカスタマーマネージドアプリケーションを設定する方法については、そのアプリケーションのドキュメントを参照してください。

信頼できるトークン発行者の構成設定

次のセクションでは、信頼できるトークン発行者をセットアップして使用するために必要な設定について説明します。

トピック

- OIDC 検出エンドポイント URL (発行者 URL)
- 属性マッピング
- Aud クレーム

OIDC 検出エンドポイント URL (発行者 URL)

IAM アイデンティティセンターコンソールに信頼できるトークン発行者を追加するときは、OIDC ディスカバリーエンドポイント URL を指定する必要があります。この URL は通常、その相対 URL である `/.well-known/openid-configuration` で呼ばれます。IAM アイデンティティセンターコンソールでは、この URL は発行者 URL と呼ばれます。

> **Note**
>
> 検出エンドポイントの URL は、 まで貼り付ける必要があります`.well-known/openid-configuration`。`.well-known/openid-configuration` が URL に含まれている場合、信頼できるトークン発行者の設定は機能しません。IAM Identity Center はこの URL を検証しないため、URL が正しく形成されていない場合、信頼できるトークン発行者の設定は通知なしで失敗します。

IAM アイデンティティセンターはこの URL を使用して、信頼できるトークン発行者に関する追加情報を取得します。例えば、IAM アイデンティティセンターは、この URL を使用して、信頼できるトークン発行者が生成するトークンの検証に必要な情報を取得します。IAM アイデンティティセンターに信頼できるトークン発行者を追加するときは、この URL を指定する必要があります。URL を確認するには、アプリケーション用のトークンの生成に使用する OAuth 2.0 認証サーバープロバイダーのドキュメントを参照するか、プロバイダーに直接問い合わせて支援を求めてください。

属性マッピング

属性マッピングにより、IAM アイデンティティセンターは、信頼できるトークン発行者が発行したトークンに示されているユーザーを IAM アイデンティティセンター内の 1 人のユーザーと照合できます。IAM アイデンティティセンターに信頼できるトークン発行者を追加するときは、属性マッピングを指定する必要があります。この属性マッピングは、信頼できるトークン発行者が生成するトークンのクレームに使用されます。このクレームの値は IAM アイデンティティセンターの検索に使用されます。この検索では、指定された属性を使用して IAM アイデンティティセンター内の 1 人のユーザーを取得します。このユーザーは AWS内のユーザーとして使用されます。選択したクレームは、IAM アイデンティティセンターID ストア内の使用可能な属性の固定リスト内の 1 つの属性にマッピングする必要があります。IAM アイデンティティセンターID ストア属性の、ユーザー名、E メール、外部 ID のいずれか一つを選択できます。IAM アイデンティティセンターで指定する属性の値は、ユーザーごとに一意である必要があります。

Aud クレーム

Aud クレームは、トークンの対象となる対象者 (受信者) を識別します。アクセスをリクエストするアプリケーションが IAM アイデンティティセンターにフェデレーションされていない ID プロバイダーを通じて認証される場合、その ID プロバイダーを信頼できるトークン発行者として設定する必要があります。アクセスリクエストを受信するアプリケーション (受信側アプリケーション) は、信頼できるトークン発行者が生成したトークンを IAM アイデンティティセンターが生成したトークンと交換する必要があります。

信頼できるトークン発行者に登録されている受信側アプリケーションの aud クレーム値を取得する方法については、信頼できるトークン発行者のドキュメントを参照するか、信頼できるトークン発行者の管理者に支援を問い合わせてください。

信頼できるトークン発行者の設定

IAM アイデンティティセンターの外部認証を行うアプリケーションに対し、信頼できる ID を伝播きるようにするには、1 人以上の管理者が、信頼できるトークン発行者を設定する必要があります。信頼できるトークン発行者とは、リクエストを開始するアプリケーション (リクエスト元アプリケーション) にトークンを発行する OAuth 2.0 認証サーバーです。トークンは、これらのアプリケーションがユーザーに代わって受信側アプリケーション (AWS サービス) へのリクエストを開始することを承認します。

トピック

- 管理者の役割と責任の調整
- 信頼できるトークン発行者を設定するタスク
- IAM アイデンティティセンターコンソールに信頼できるトークン発行者を追加する方法
- IAM アイデンティティセンターコンソールで信頼できるトークン発行者の設定を表示または編集する方法
- 信頼できるトークン発行者を使用するアプリケーションのセットアッププロセスおよびリクエストフロー

管理者の役割と責任の調整

場合によっては、単独の管理者が、信頼できるトークン発行者の設定に必要なすべてのタスクを実行することもあります。複数の管理者がこれらのタスクを実行する場合は、緊密な調整が必要です。次の表は、複数の管理者が連携して信頼できるトークン発行者を設定し、それを使用するように AWS サービスを設定する方法を示しています。

> **Note**
>
> アプリケーションは、IAM Identity Center と統合され、信頼できる ID の伝播をサポートする任意の AWS サービスにすることができます。

詳細については、「信頼できるトークン発行者を設定するタスク」を参照してください。

[Role] (ロール)	これらのタスクを実行する	コーディネートする
IAM アイデンティティセンター管理者	外部 IdP を、信頼できるトークン発行者として、IAM アイデンティティセンターコンソールに追加します。 IAM アイデンティティセンターと外部 IdP 間の正しい属性マッピングを設定するのに役立ちます。 信頼できるトークン発行者が IAM Identity Center コンソールに追加されると、 AWS サービス管理者に通知します。	外部 IdP (信頼できるトークン発行者) 管理者 AWS サービス管理者
外部 IdP (信頼できるトークン発行者) 管理者	トークンを発行するように外部 IdP を設定します。 IAM アイデンティティセンターと外部 IdP 間の正しい属性マッピングを設定するのに役立ちます。 対象者名 (Aud 要求) を AWS サービス管理者に提供します。	IAM アイデンティティセンター管理者 AWS サービス管理者
AWS サービス管理者	AWS サービスコンソールで信頼できるトークン発行者を確認します。信頼できるトークンの発行者は、IAM アイデンティティセン	IAM アイデンティティセンター管理者 外部 IdP (信頼できるトークン発行者) 管理者

[Role] (ロール)	これらのタスクを実行する	コーディネートする
	ター管理者が IAM アイデンティティセンターコンソールにそれを追加すると、 AWS サービスコンソールに表示できるようになります。 信頼できるトークン発行者を使用するように AWS サービスを設定します。	

信頼できるトークン発行者を設定するタスク

信頼できるトークン発行者を設定するには、IAM アイデンティティセンター管理者、外部 IdP (信頼できるトークン発行者) 管理者、およびアプリケーション管理者が次のタスクを完了する必要があります。

> **Note**
>
> アプリケーションは、IAM Identity Center と統合され、信頼できる ID の伝播をサポートする任意の AWS サービスにすることができます。

1. 信頼できるトークン発行者を IAM アイデンティティセンターに追加する — IAM アイデンティティセンターの管理者は、IAM アイデンティティセンターコンソールまたは API を使用して信頼できるトークン発行者を追加します。この設定では、以下を指定する必要があります。
   - 信頼できるトークン発行者の名前
   - OIDC ディスカバリーエンドポイント URL (IAM アイデンティティセンターコンソールでは、この URL は 発行者 URL と呼ばれます)。
   - ユーザー検索用の属性マッピング。この属性マッピングは、信頼できるトークン発行者が生成するトークンのクレームに使用されます。このクレームの値は IAM アイデンティティセンターの検索に使用されます。検索では、指定された属性を使用して IAM アイデンティティセンター内の 1 人のユーザーを取得します。
2. AWS サービスを IAM Identity Center に接続する – AWS サービス管理者は、アプリケーションのコンソールまたはアプリケーション APIsに接続する必要があります。

信頼できるトークン発行者が IAM Identity Center コンソールに追加されると、 AWS サービスコンソールにも表示され、 AWS サービス管理者が選択できます。

3. トークン交換の使用を設定する – AWS サービスコンソールでは、 AWS サービス管理者は、信頼できるトークン発行者が発行したトークンを受け入れるように AWS サービスを設定します。これらのトークンは IAM アイデンティティセンターによって生成されたトークンと交換されます。これには、ステップ 1 で信頼されたトークン発行者の名前と、 AWS サービスに対応する Aud クレーム値を指定する必要があります。

   信頼できるトークン発行者は、発行するトークンに Aud クレーム値を入れて、そのトークンが AWS サービスによる使用を目的としていることを示します。この値を取得するには、信頼できるトークン発行者の管理者に問い合わせてください。

IAM アイデンティティセンターコンソールに信頼できるトークン発行者を追加する方法

複数の管理者がいる組織では、このタスクは IAM アイデンティティセンター管理者が実行します。IAM アイデンティティセンター管理者である場合は、信頼できるトークン発行者として使用する外部 IdP を選択する必要があります。

IAM アイデンティティセンターコンソールに信頼できるトークン発行者を追加するには

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. 「設定」 ページで、「認証」タブを選択します。
4. [信頼できるトークン発行者] で [信頼できるトークン発行者を作成] を選択します。
5. 「信頼できるトークンを発行するための外部 IdP を設定する」ページの「信頼できるトークン発行者の詳細」で、次の操作を行います。

   - 発行者 URL には、信頼できる ID の伝播用にトークンを発行する外部 IdP の OIDC 検出 URL を指定します。検出エンドポイントの URL は、 を使用するまで指定する必要があります`.well-known/openid-configuration`。外部 IdP の管理者がこの URL を提供できます。

   > **Note**
   >
   > 注: この URL は、信頼できる ID の伝播用に発行されたトークンの発行者 (iss) クレームの URL と一致する必要があります。

- [信頼できるトークンの発行者名] には、IAM アイデンティティセンターとアプリケーションコンソールで、この信頼できるトークン発行者を識別する名前を入力します。

6. [マップ属性] で、次の操作を行います。

   - [ID プロバイダー属性] では、IAM アイデンティティセンターID ストアの属性にマップする属性をリストから選択します。
   - [IAM アイデンティティセンター属性] では、属性マッピングに対応する属性を選択します。

7. [タグ (オプション)] で [新しいタグを追加] を選択し、[キー] と任意で [値 (オプション)] の値を指定します。

   タグの詳細については、「AWS IAM Identity Center リソースのタグ付け」を参照してください。

8. [信頼できるトークン発行者を作成] を選択します。
9. 信頼できるトークン発行者の作成が完了したら、アプリケーション管理者に連絡して信頼できるトークン発行者の名前を伝えて、管理者が信頼できるトークン発行者が該当するコンソールに表示されることを確認できるようにします。
10. アプリケーション管理者は、該当するコンソールでこの信頼できるトークン発行者を選択する必要があります。これにより、信頼できる ID が伝播されるように構成されたアプリケーションからユーザーがアプリケーションにアクセスできるようになります。

IAM アイデンティティセンターコンソールで信頼できるトークン発行者の設定を表示または編集する方法

IAM アイデンティティセンターコンソールに信頼できるトークン発行者を追加すると、関連設定を表示および編集できます。

信頼できるトークン発行者の設定を編集する予定がある場合は、その信頼できるトークン発行者を使用するように設定されているアプリケーションにユーザーがアクセスできなくなる可能性があることに注意してください。ユーザーアクセスを妨げないように、設定を編集する前に、信頼できるトークン発行者を使用するように構成されているアプリケーションの管理者と連絡を取ることをお勧めします。

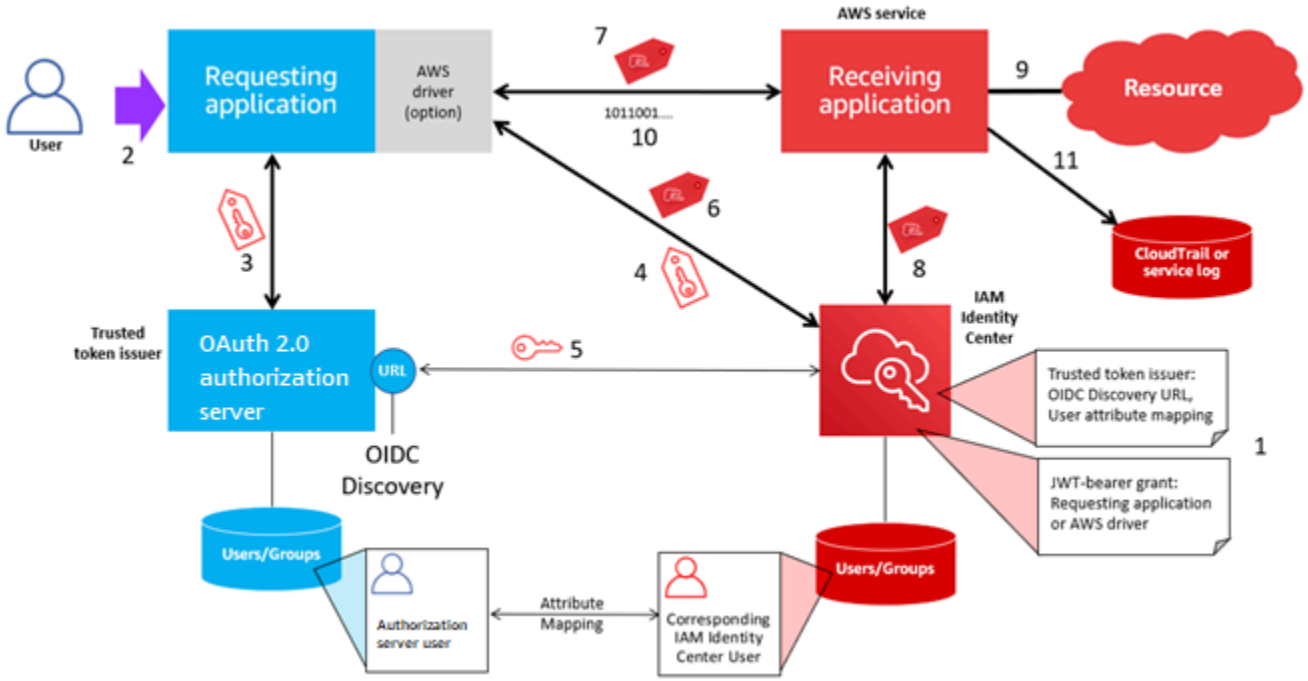
IAM アイデンティティセンターコンソールで信頼できるトークン発行者の設定を表示または編集するには

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。

3. 「設定」 ページで、「認証」タブを選択します。
4. [信頼できるトークン発行者] で、表示または編集する信頼できるトークン発行者を選択します。
5. [Actions] (アクション) を選択して、[Edit] (編集) を選択します。
6. [信頼できるトークンの発行者を編集] ページで、必要に応じて設定を表示または編集します。信頼できるトークンの発行者名、属性マッピング、およびタグを編集することができます。
7. [変更を保存] を選択します。
8. [信頼できるトークン発行者を編集] ダイアログボックスに、変更を加えるかどうかを確認するメッセージが表示されます。[確認] を選択します。

信頼できるトークン発行者を使用するアプリケーションのセットアッププロセスおよびリクエストフロー

このセクションでは、信頼できるトークン発行者を使用して信頼できる ID の伝播を行うアプリケーションのセットアッププロセスとリクエストフローについて説明します。次の図は、このプロセスの概要を示しています。



次の手順で、このプロセスに関する追加情報を提供します。

1. 信頼できるトークン発行者を使用するように IAM Identity Center と受信側 AWS マネージドアプリケーションをセットアップします。詳細については、「信頼できるトークン発行者を設定するタスク」を参照してください。

2. リクエストフローは、ユーザーがリクエスト元のアプリケーションを開くと開始されます。
3. リクエスト元のアプリケーションは、信頼できるトークン発行者からトークンをリクエストして、受信側の AWS マネージドアプリケーションへのリクエストを開始します。ユーザーがまだ認証されていない場合、このプロセスによって認証フローがトリガーされます。このトークンには次の情報が含まれます。
   - ユーザーのサブジェクト (Sub)。
   - IAM アイデンティティセンターが IAM アイデンティティセンター内の対応するユーザーを検索するために使用する属性。
   - 信頼できるトークン発行者が受信側の AWS マネージドアプリケーションに関連付ける値を含む対象者 (Aud) クレーム。他のクレームが存在する場合、これらは IAM アイデンティティセンターでは使用されません。
4. リクエスト元のアプリケーションまたは使用する AWS ドライバーは、トークンを IAM Identity Center に渡し、トークンを IAM Identity Center によって生成されたトークンと交換するようリクエストします。 AWS ドライバーを使用する場合は、このユースケースに合わせてドライバーを設定する必要がある場合があります。詳細については、関連する AWS マネージドアプリケーションのドキュメントを参照してください。
5. IAM アイデンティティセンターは OIDC Discovery エンドポイントを使用して、トークンの信頼性を検証するために使用できるパブリックキーを取得します。次に IAM アイデンティティセンターは次の処理を行います。
   - このトークンを検証します。
   - Identity Center ディレクトリを検索します。これを行うには、IAM アイデンティティセンターはトークンで指定されたマッピングされた属性を使用します。
   - ユーザーが受信側のアプリケーションにアクセスする権限を持っていることを確認します。AWS マネージドアプリケーションがユーザーとグループへの割り当てを要求するように設定されている場合、ユーザーはアプリケーションへの直接またはグループベースの割り当てを持っている必要があります。そうでない場合、リクエストは拒否されます。 AWS マネージドアプリケーションがユーザーとグループの割り当てを必要としないように設定されている場合、処理は続行されます。

> **Note**
>
> AWS サービスには、ユーザーとグループに割り当てが必要かどうかを決定するデフォルト設定があります。これらのアプリケーションを信頼できる ID の伝播と組み合わせて使用する予定の場合は、これらのアプリケーションの [割り当ては必須です] 設定を変更しないことをお勧めします。特定のアプリケーションリソースへのユーザーアクセス

を許可するきめ細かいアクセス許可を設定した場合でも、[割り当ては必須です] 設定を変更すると、これらのリソースへのユーザーアクセスが中断されるなど、予期しない動作が発生する可能性があります。

- リクエスト元のアプリケーションが、受信側の AWS マネージドアプリケーションに有効なスコープを使用するように設定されていることを確認します。

6. 前の検証ステップが成功すると、IAM アイデンティティセンターは新しいトークンを作成します。新しいトークンは、IAM Identity Center の対応するユーザーのアイデンティティ、受信側の AWS マネージドアプリケーションの対象者 (Aud)、受信側の AWS マネージドアプリケーションにリクエストを行うときにリクエスト元のアプリケーションが使用できるスコープを含む不透明な (暗号化された) トークンです。
7. リクエスト元のアプリケーションまたはそれが使用するドライバーは、受信アプリケーションへのリソースリクエストを開始し、IAM アイデンティティセンターが生成したトークンを受信アプリケーションに渡します。
8. 受信側のアプリケーションは IAM アイデンティティセンターを呼び出して、ユーザーの ID とトークンにエンコードされたスコープを取得します。Identity Center ディレクトリからユーザー属性またはユーザーのグループメンバーシップを取得するようにリクエストする場合もあります。
9. 受信側のアプリケーションは、その認証設定を使用して、リクエストされたアプリケーションリソースへのアクセスがユーザーに許可されているかどうかを判断します。
10. リクエストされたアプリケーションリソースへのアクセスがユーザーに許可されている場合、受信側のアプリケーションはそのリクエストに応答します。
11. ユーザーの ID、ユーザーに代わって実行されるアクション、および受信側のアプリケーションログと CloudTrailイベントに記録されたその他のイベント。この情報を記録する具体的な方法は、アプリケーションによって異なります。

IAM Identity Center 証明書の管理

IAM アイデンティティセンターは、証明書を使用して IAM アイデンティティセンターとアプリケーションのサービスプロバイダーとの間の SAML 信頼関係をセットアップします。IAM Identity Center でアプリケーションを追加すると、セットアップ時にそのアプリケーションで使用する IAM Identity Center 証明書が自動的に作成されます。デフォルトでは、この自動生成された IAM Identity Center 証明書の有効期間は 5 年間です。

IAM Identity Center の管理者として、特定のアプリケーションのために、古い証明書を新しいものに置き換える必要がある場合があります。例えば、証明書の有効期限が近づいている場合、証明書を交

換する必要があります。古い証明書を新しい証明書に置き換えるプロセスは、証明書のローテーションと呼ばれています。

トピック

証明書をローテーションする前の注意事項

IAM Identity Center で証明書をローテーションするプロセスを開始する前に、以下について検討してください。

- 認証ローテーションプロセスでは、IAM Identity Center とサービスプロバイダーの間の信頼関係を再構築する必要があります。信頼を再確立するには、IAM Identity Center 証明書の交代 に記載されている手順を行います。
- サービスプロバイダーの証明書を更新すると、信頼関係が正常に再構築されるまで、ユーザーに一時的なサービス障害が発生する場合があります。このオペレーションは、ピーク時を可能な限り避けて慎重に計画してください。

IAM Identity Center 証明書の交代

IAM Identity Center 証明書のローテーションは、以下の複数のステップで行われます。

- 新しい証明書を生成する
- 新しい証明書をサービスプロバイダのウェブサイトに追加する
- 新しい証明書をアクティブにする
- 非アクティブな証明書を削除する

特定のアプリケーションの証明書ローテーションプロセスを完了するには、次の手順をすべて行います。

ステップ 1: 新しい証明書を生成する

生成した新しい IAM Identity Center 証明書は、以下のプロパティを使用するように設定できます。

- 有効期間 — 新しい IAM Identity Center 証明書の有効期限が切れるまでの期間 (月単位) を指定します。
- キーサイズ — キーが暗号アルゴリズムで使用するビット数を決定します。この値は、1024 ビット RSA または 2048 ビット RSA のいずれかに設定できます。暗号化におけるキーサイズの仕組みに関する一般情報については、「Key size」(キーサイズ) を参照してください。
- アルゴリズム — SAML アサーション/レスポンスの署名時に IAM Identity Center が使用するアルゴリズムを指定します。この値は、サービスプロバイダーが SHA-1 を必要とする場合を除き、可能な場合は SHA-256 を使用して SHA-1 または SHA-256. AWS recommends のいずれかに設定できます。 SHA-1 暗号化アルゴリズムの仕組みに関する一般情報については、「Public-key cryptography」(パブリックキー暗号) を参照してください。

1. IAM Identity Center コンソール を開きます。
2. [Applications] (アプリケーション) を選択します。
3. アプリケーションのリストで、新しい証明書を生成するアプリケーションを選択します。
4. [Application details] (アプリケーションの詳細) ページで、[Settings] (設定) タブをクリックします。[IAM アイデンティティセンターのメタデータ] で、[証明書を管理] を選択します。[構成] タブがない場合や、構成設定が使用できない場合は、このアプリケーションの証明書をローテーションする必要はありません。
5. [IAM Identity Center 証明書] ページで、[新しい証明書を生成] を選択します。
6. [新しい IAM Identity Center 証明書を生成する] ダイアログボックスで、[有効期間]、[アルゴリズム]、[キーサイズ] に適切な値を指定します。次に [Generate] (生成) をクリックします。

ステップ 2: サービスプロバイダのウェブサイトを更新する。

以下の手順で、アプリケーションのサービスプロバイダーとの信頼関係を再構築します。

> **Important**
>
> 新しい証明書をサービスプロバイダーにアップロードすると、ユーザーが認証を受けられなくなる可能性があります。この問題を解決するには、次のステップの説明にあるとおり、新しい証明書をアクティブに設定します。

1. IAM Identity Center コンソールで、先ほど新しい証明書を生成したアプリケーションをクリックします。

2. [Application details] (アプリケーションの詳細) ページで、[Edit configuration] (設定の変更) タブをクリックします。
3. [View instructions] (手順を表示する) をクリックし、特定のアプリケーションサービスプロバイダーのウェブサイトの指示に従って、新しく生成された証明書を追加します。

ステップ 3: 新しい証明書をアクティブにする。

アプリケーションには、最大 2 つの証明書を割り当てることができます。IAM アイデンティティセンターは、すべての SAML アサーションに署名するためにアクティブに設定されている証明書を使用します。

1. IAM Identity Center コンソール を開きます。
2. [Applications] (アプリケーション) を選択します。
3. アプリケーションのリストで [your application] (お客様のアプリケーション) をクリックします。
4. [Application details] (アプリケーションの詳細) ページで、[Settings] (設定) タブをクリックします。[IAM Identity Center のメタデータ] で [証明書の管理] を選択します。
5. [IAM Identity Center 証明書] ページで、アクティブに設定したい証明書を選択し、[アクション] をクリックし、そして、[アクティブとして設定] をクリックします。
6. [Set the selected certificate as active] (選択した証明書をアクティブにする) ダイアログで、証明書をアクティブにすると信頼関係の再構築が必要になることを確認して、[Make active] (アクティブにする) をクリックします。

ステップ 4: 古い証明書を削除します。

以下の手順で、アプリケーションの証明書ローテーション処理を行います。削除できるのは、Inactive (無効) 状態の証明書のみです。

1. IAM Identity Center コンソール を開きます。
2. [Applications] (アプリケーション) を選択します。
3. アプリケーションのリストで [your application] (お客様のアプリケーション) をクリックします。
4. アプリケーションの詳細ページで、[Configuration] (構成) タブを選択します。[IAM Identity Center のメタデータ] で [証明書の管理] を選択します。

5. [IAM Identity Center 証明書] ページで、削除する証明書を選択します。[Actions] (アクション) を選択してから、[Delete] (削除) を選択します。
6. [Delete certificate] (証明書の削除) ダイアログボックスで、[Delete] (削除) をクリックします。

証明書の有効期限切れステータスインジケーター

アプリケーションのプロパティの [Applications] (アプリケーション) ページでは、色付きのステータスインジケータのアイコンが表示されることがあります。これらのアイコンは、リストの各証明書の横にある [Expires on] (有効期限) 列に表示されます。以下は、IAM Identity Center が各証明書に対してどのアイコンを表示するかを決定するための基準です。

- 赤 — 証明書が現在期限切れであることを示します。
- 黄 — 証明書の有効期限が 90 日以下であることを示します。
- 緑 — 証明書が現在有効であり、少なくとも 90 日間有効であることを示します。

証明書の現在のステータスを確認するには

1. IAM Identity Center コンソール を開きます。
2. [Applications] (アプリケーション) を選択します。
3. アプリケーションの一覧で、[Expires on] (有効期限) 列に表示されている証明書のステータスを確認します。

IAM アイデンティティセンターコンソールのアプリケーションプロパティを設定する

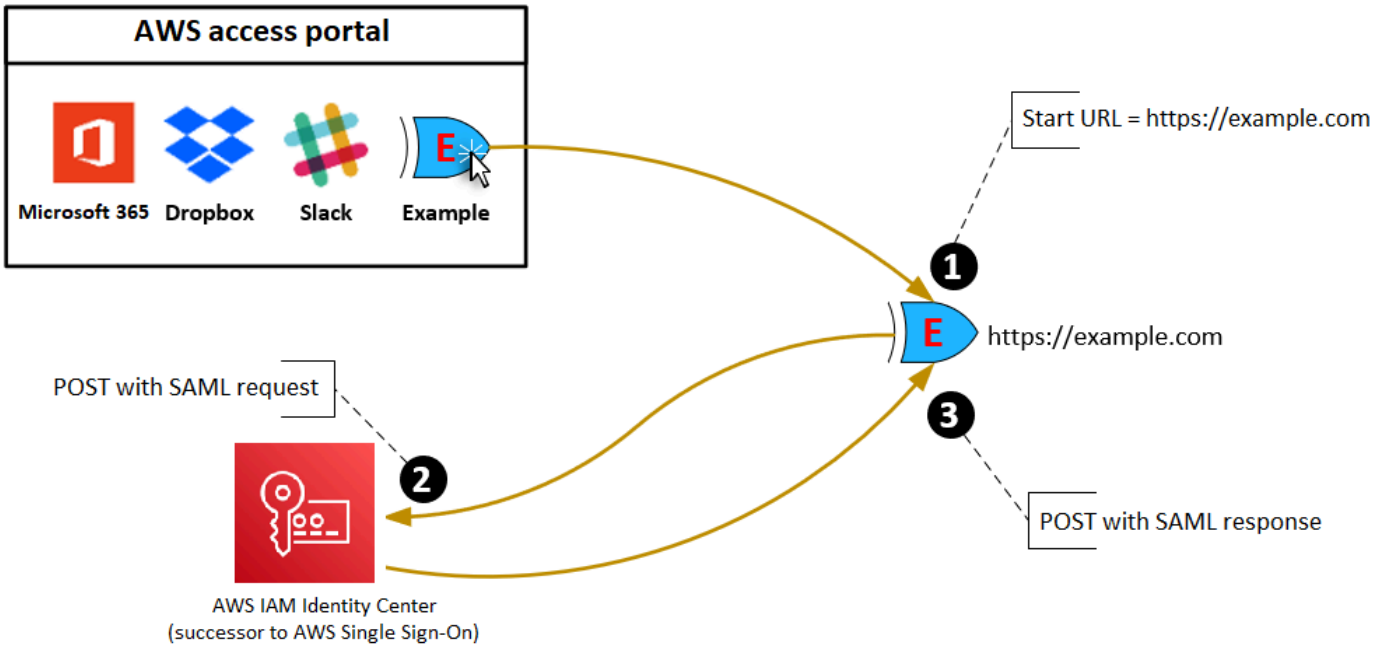
IAM Identity Center では、アプリケーションの開始 URL、リレーステート、セッション時間を設定することで、ユーザーエクスペリエンスをカスタマイズできます。

アプリケーション開始 URL

アプリケーション開始 URL を使用して、アプリケーションでフェデレーションプロセスを開始できます。一般的な用途は、サービスプロバイダー (SP) 開始バインディングのみをサポートするアプリケーション用です。

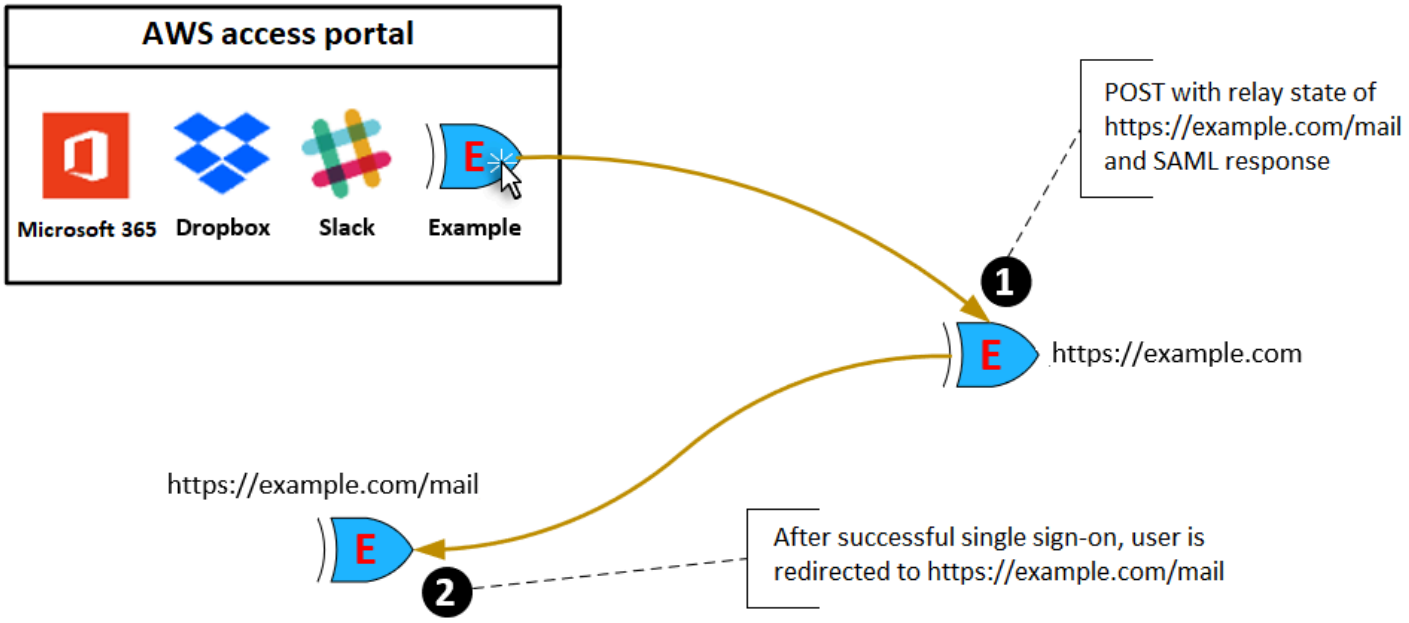
以下のステップと図は、ユーザーが AWS アクセスポータルでアプリケーションを選択したときのアプリケーション開始 URL の認証ワークフローを示しています。

1. ユーザーのブラウザは、アプリケーション開始 URL (この場合は https://example.com) の値を使用して認証リクエストをリダイレクトします。
2. アプリケーションは、IAM Identity Center にSAMLRequest付きのHTMLPOSTを送信します。
3. 次に IAM Identity Center は HTMLPOST を SAMLResponse でアプリケーションに送り返します。



リレーステート

フェデレーション認証プロセス中に、リレーステートはアプリケーション内でユーザーをリダイレクトします。SAML 2.0 の場合、この値は、変更されずにアプリケーションに渡されます。アプリケーションのプロパティ設定が完了すると、IAM Identity Center が SAML レスポンスとともにリレーステート値をアプリケーションに送信します。



セッション期間

セッション期間は、アプリケーションのユーザー セッションが有効な時間の長さです。SAML 2.0 では、これは、SAML アサーションの要素 `saml2:AuthNStatement` の `SessionNotOnOrAfter` の日付を設定するために使用されます。

セッション期間は次のいずれかの方法でアプリケーションによって解釈されます。

- アプリケーションはこれを使用して、ユーザーのセッションに許可される最大時間を決定できます。アプリケーションによっては、より短い時間のユーザーセッションを生成する可能性があります。これは、設定されたセッションの長さよりも短い期間のユーザーセッションのみをアプリケーションがサポートする場合に発生する可能性があります。
- アプリケーションはこれを正確な期間として使用でき、管理者に値の設定を許可しない場合があります。これは、アプリケーションが特定のセッションの長さのみをサポートするときに発生する可能性があります。

セッション期間の使用の詳細については、ご使用のアプリケーションのドキュメントを参照してください。

IAM Identity Center コンソールでアプリケーションへのユーザーアクセスを割り当てます。

アプリケーションカタログ内の SAML 2.0 アプリケーションまたはカスタム SAML 2.0 アプリケーションへのシングルサインオンアクセスをユーザーに割り当てることができます。

グループ割り当てに関する考慮事項:

- アクセス権をグループに直接割り当てます。アクセス権限の管理をシンプルにするためには、個々のユーザーではなくグループに直接アクセスを割り当てることをお勧めします。グループを使用すると、個々のユーザーにこれらのアクセス権限を適用するのではなく、ユーザーグループに対してアクセス権限を付与または拒否できます。ユーザーが別の組織に異動した場合、そのユーザーを別のグループに移動させるだけです。その後、ユーザーは新しい組織に必要な権限を自動的に受け取ります。
- ネストされたグループはサポートされません。アプリケーションへのアクセス許可をユーザーに割り当てる場合、IAM Identity Center はネストされたグループへのユーザーの追加はサポートしていません。ユーザーがネストされたグループに追加されると、サインイン時に「アプリケーションがありません」というメッセージが表示される場合があります。割り当ては、ユーザーが属している直属のグループに対して行われなければなりません。

ユーザーまたはグループにアプリケーションへのアクセスを割り当てるには

> **Important**
>
> AWS マネージドアプリケーションの場合は、関連するアプリケーションコンソール内から直接、または APIsを介してユーザーを追加する必要があります。

1. IAM Identity Center コンソールを開きます。

   > **Note**
   >
   > でユーザーを管理する場合は AWS Managed Microsoft AD、次のステップに進む前に、IAM Identity Center コンソールで AWS Managed Microsoft AD ディレクトリがある AWS リージョンを使用していることを確認してください。

2. [Applications] (アプリケーション) を選択します。

3. アプリケーションのリストで、アクセスを割り当てるアプリケーション名を選択します。
4. アプリケーションの詳細ページの [割り当てられたユーザー] セクションで、[割り当てられたユーザー] をクリックします。
5. [Assign users] (ユーザーの割り当て) ダイアログボックスにユーザー名またはグループ名を入力します。ユーザーやグループを検索することもできます。複数のユーザーまたはグループを指定するには、検索結果に表示される該当するアカウントを選択します。
6. [ユーザーの割り当て] を選択します。

IAM Identity Center コンソールでユーザーアクセスを削除します。

アプリケーションカタログの SAML 2.0 アプリケーションまたはカスタム SAML 2.0 アプリケーションへのユーザーアクセスを削除するには、この手順を実行します。

アプリケーションへのユーザーアクセスを削除するには

1. IAM Identity Center コンソール を開きます。
2. [Applications] (アプリケーション) を選択します。
3. アプリケーションのリストで、ユーザーアクセスを削除するアプリケーションを選択します。
4. アプリケーションの詳細ページの [割り当てられたユーザー] セクションで、削除するユーザーまたはグループを選択してから、[削除] を選択します。
5. [Remove access] (アクセスの削除) ダイアログボックスで、ユーザー名またはグループ名を確認します。次に、[Remove access] (アクセスの削除) を選択します。

アプリケーションの属性を IAM Identity Center の属性にマップする

一部のサービスプロバイダーでは、ユーザーのサインインに関する追加のデータを渡すためにカスタム SAML アサーションが必要です。その場合は、以下の手順を使用して、アプリケーションのユーザー属性を IAM Identity Center の対応する属性にマップする方法を指定します。

アプリケーションの属性を IAM Identity Center の属性にマップするには

1. IAM Identity Center コンソール を開きます。
2. [Applications] (アプリケーション) を選択します。
3. アプリケーションのリストで、属性をマップするアプリケーションを選択します。

4. アプリケーション詳細ページで [アクション] を選択し、[属性マッピングを編集] を選択します。
5. [新規属性マッピングの追加] を選択します。
6. 最初のテキストボックスに、アプリケーションの属性を入力します。
7. 2 番目のテキストボックスに、アプリケーションの属性にマップする IAM Identity Center の属性を入力します。たとえば、アプリケーションの属性 **`Username`** を IAM Identity Center のユーザー属性 **`email`** にマップできます。IAM Identity Center で許可されるユーザー属性のリストについては、「AWS Managed Microsoft AD　ディレクトリの属性マッピング」の表を参照してください。
8. この一覧の 3 番目の列で、メニューから属性に該当する形式をクリックします。
9. [変更を保存] を選択します。

復元力設計とリージョンごとの動作

IAM Identity Center サービスはフルマネージド型で、Amazon S3 や Amazon EC2 などの可用性と耐久性に優れた AWS サービスを使用します。アベイラビリティーゾーンに障害が発生した場合でも可用性を確保するため、IAM Identity Center は複数のアベイラビリティーゾーンにわたって運用されています。IAM アイデンティティセンターの可用性設計目標については、「信頼性の柱のガイド」の「付録 A: 一部の AWS サービスの可用性を考慮した設計」を参照してください。

AWS Organizations 管理アカウントで IAM Identity Center を有効にします。これは、IAM Identity Center がすべての AWS アカウント のロールをプロビジョニング、プロビジョニング解除、更新できるようにするために必要です。IAM Identity Center を有効にすると、現在選択されている AWS リージョン にデプロイされます。特定の AWS リージョン にデプロイする場合は、IAM Identity Center を有効にする前にリージョンの選択を変更してください。

> **Note**
>
> IAM Identity Center は、プライマリリージョンからのみアクセス権限セットとアプリケーションへのアクセスを制御します。IAM Identity Center が 1 つのリージョンで運用されている場合は、アクセス制御に関連するリスクを考慮することをお勧めします。

IAM Identity Center はサービスを有効にしたリージョンからのアクセスを決定しますが、AWS アカウント はグローバルです。つまり、ユーザーが IAM Identity Center にサインインした後は、IAM Identity Center を介してアクセスすればAWS アカウント、どのリージョンでも操作できるようになります。ただし SageMaker、Amazon などのほとんどのAWSマネージドアプリケーションは、ユーザーがこれらのアプリケーションに対する認証とアクセスの割り当てを行うために、IAM Identity Center と同じリージョンにインストールする必要があります。IAM Identity Center でアプリケーションを使用する場合のリージョンの制約については、アプリケーションのドキュメントを参照してください。

IAM Identity Center を使用して、アプリケーションが構築されているプラットフォームやクラウドに関係なく、パブリック URL を介してアクセス可能な SAML ベースのアプリケーションへのアクセスを認証および承認することもできます。

組織インスタンスに接続されていない 2 番目の分離されたコントロールポイントが作成されるため、復元性を実装する手段として IAM アイデンティティセンターのアカウントインスタンス を使用することはお勧めしません。

AWS Management Console への緊急アクセスを設定する

IAM Identity Center は可用性の高い AWS インフラストラクチャを基盤として構築されており、Availability Zone アーキテクチャを使用して単一障害点を排除しています。万一 IAM Identity Center や のAWS リージョン中断が発生した場合に保護を強化するために、 への一時的なアクセスを提供するために使用できる設定を設定することをお勧めしますAWS Management Console。

コンテンツ

概要

AWS により以下ができます。

- サードパーティ IdP を IAM Identity Center に接続します。
- SAML 2.0 ベースのフェデレーション を使用して、サードパーティーの IdP を個人 AWS アカウント に接続します。

IAM Identity Center を使用している場合は、これらの機能を使用して、以下のセクションで説明する緊急アクセス設定を作成できます。この設定により、IAM Identity Center を AWS アカウント アクセスのメカニズムとして使用できるようになります。IAM Identity Center が停止した場合、緊急時の操作を行うユーザーは、アカウントへのアクセスに使用するのと同じ認証情報を使用して、ダイレクトフェデレーションを通じて AWS Management Console にサインインできます。この設定は、IAM Identity Center は使用できないが、IAM データプレーンと外部 ID プロバイダー (IdP) は使用できる場合に機能します。

> **Important**
>
> 必要な IAM ロールを作成するためのアクセスも中断されると設定を作成できないため、中断が発生する前にこの設定をデプロイすることをお勧めします。また、この設定を定期的にテストして、IAM Identity Center が中断された場合の対処方法をチームが理解できるようにしてください。

緊急アクセス設定の概要

緊急アクセスを設定するには、次のタスクを完了する必要があります。

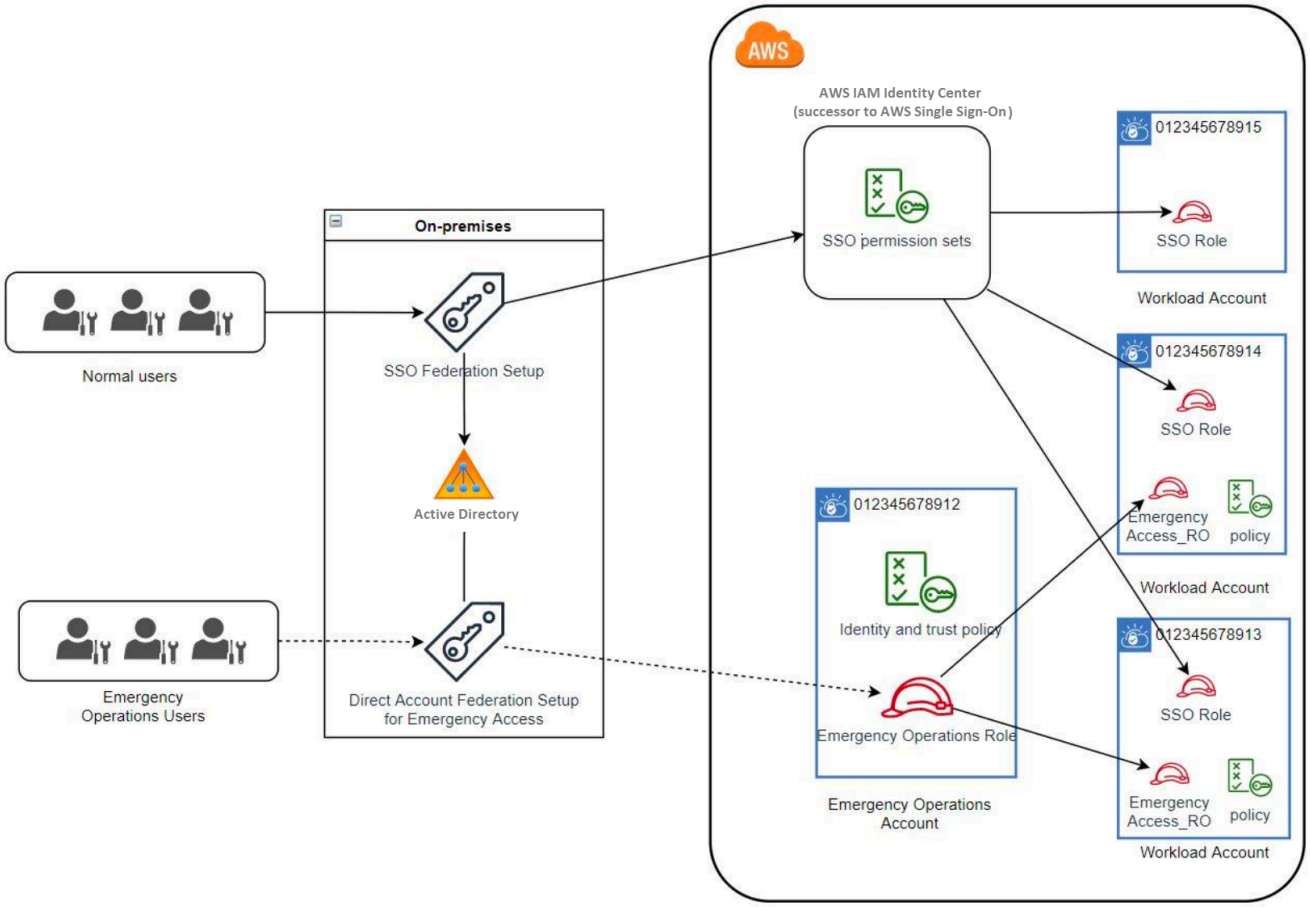
1. AWS Organizationsで、組織の緊急対応アカウントを作成してください。
2. SAML 2.0 ベースのフェデレーションを使用して IdP を緊急対応アカウントに接続します。
3. 緊急対応アカウントで、サードパーティーの ID プロバイダーフェデレーション用のロールを作成します。また、各ワークロードアカウントに、必要な権限を持つ緊急対応ロールを作成します。
4. 緊急対応アカウントで作成した IAM ロールに、ワークロードアカウントへのアクセスを委任します。緊急対応アカウントへのアクセスを許可するには、メンバーなしで IdP に緊急対応グループを作成します。
5. IdP に SAML 2.0 フェデレーションのAWS Management Consoleへのアクセスを有効にするルールを作成して、IdP 内の緊急対応グループが、緊急対応ロールを使用できるようにします。

IdP の緊急対応グループにはメンバーがいないため、通常の運用中は誰も緊急対応アカウントにアクセスできません。IAM Identity Center に障害が発生した場合は、IdP を使用して信頼できるユーザーを IdP の緊急対応グループに追加します。その後、これらのユーザーは IdP にサインインして AWS Management Console に移動し、緊急対応アカウントの緊急対応ロールを引き受けることができます。そこから、これらのユーザーは、運用作業を行う必要があるワークロードアカウントの緊急アクセスロールにロールを切り替える ことができます。

重要な運用上の役割を設計する方法

この設計では、IAM を介して連携する単一 AWS アカウント の役割を設定して、ユーザーが重要な運用ロールを引き受けられるようにします。重要な運用ロールには、ユーザーがワークロードアカウントで対応するロールを引き受けることを許可する信頼ポリシーがあります。ワークロードアカウントのロールは、ユーザーが重要な作業を行うために必要な権限を提供します。

次の図は、設計の概要を示しています。



アクセスモデルを計画する方法

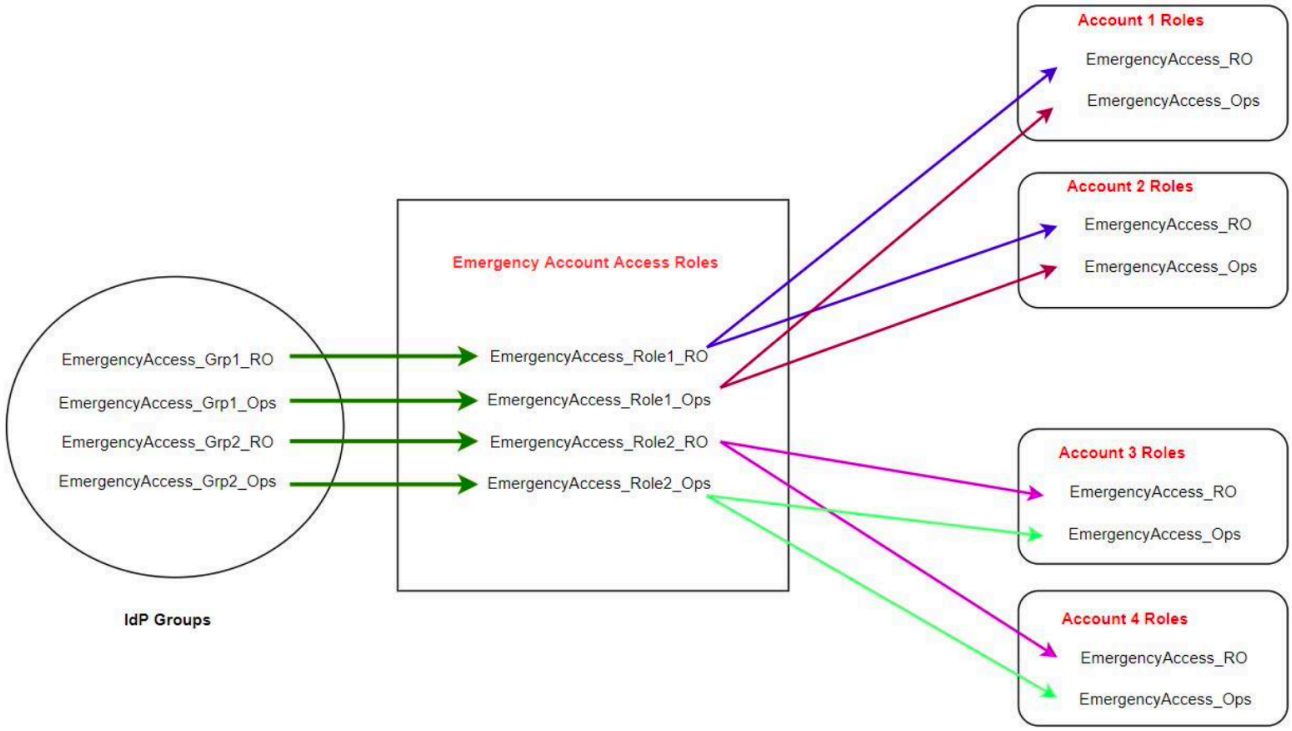
緊急アクセスを設定する前に、アクセスモデルがどのように機能するかについての計画を立ててください。このプランを作成するには、次の手順に従います。

1. IAM Identity Center の障害発生時にオペレーターによる緊急アクセスが不可欠な場所 AWS アカウント を特定します。例えば、本番アカウントはおそらく必要ですが、開発用アカウントとテスト用アカウントはそうではない場合があります。
2. このようなアカウントのコレクションに関して、アカウントに必要な具体的な重要な役割を特定してください。これらのアカウント全体で、それぞれのロールで何ができるかを一貫して定義してください。これにより、クロスアカウントロールを作成する緊急アクセスアカウントでの作業が簡素化されます。これらのアカウントでは、読み取り専用 (RO) と運用 (Ops) という 2 つの異なるロールから始めることをお勧めします。必要に応じて、さらに役割を作成し、これらの役割をセットアップ内のより明確な緊急アクセスユーザーのグループにマッピングできます。

3. IdP で緊急アクセスグループを特定して作成します。グループメンバーは、緊急アクセスロールへのアクセスを委任しているユーザーです。
4. これらのグループが緊急アクセスアカウントで引き受けることができるロールを定義します。そのためには、グループがアクセスできるロールを一覧表示するクレームを生成するルールを IdP で定義します。その後、これらのグループが緊急アクセスアカウントの「読み取り専用」または「オペレーション」のロールを引き受けることができます。これらのロールから、ワークロードアカウントの対応するロールを引き受けることができます。

緊急時のロール、アカウント、グループのマッピングを設計する方法

次の図は、緊急アクセス グループを緊急アクセスアカウントのロールにマップする方法を示しています。この図には、緊急アクセスアカウントロールがワークロードアカウント内の対応するロールにアクセスできるようにする、アカウント間ロールの信頼関係も示されています。緊急時対応計画の設計では、これらのマッピングを出発点として使用することをお勧めします。



緊急アクセス設定の作成方法

次のマッピング テーブルを使用して、緊急アクセス設定を作成します。この表は、ワークロードアカウントにおける読み取り専用 (RO) と運用 (Ops) の 2 つのロールと、対応する信頼ポリシーと権限

ポリシーを含む計画を反映しています。信頼ポリシーにより、緊急アクセスアカウントロールが個々のワークロードのアカウントロールにアクセスできるようになります。個々のワークロードアカウントロールには、そのロールが、アカウント内で実行できる操作に関するアクセス権限ポリシーもあります。アクセス権限ポリシーは、AWSマネージドポリシー でも カスタマー管理ポリシー でもかまいません。

アカウント	作成するロール	信頼ポリシー	アクセス権限ポリシー
アカウント 1	Emergency Access_RO	Emergency Access_Role1_RO	arn:aws:iam::aws:policy/ReadOnlyAccess
アカウント 1	Emergency Access_Ops	Emergency Access_Role1_Ops	arn:aws:iam::aws:policy/job-function/SystemAdministrator
アカウント 2	Emergency Access_RO	Emergency Access_Role2_RO	arn:aws:iam::aws:policy/ReadOnlyAccess
アカウント 2	Emergency Access_Ops	Emergency Access_Role2_Ops	arn:aws:iam::aws:policy/job-function/SystemAdministrator
緊急アクセスアカウント	Emergency Access_Role1_RO Emergency Access_Role1_Ops Emergency Access_Role2_RO Emergency Access_Role2_Ops	IdP	AssumeRole アカウントのロールリソースの

このマッピングプランでは、緊急アクセスアカウントには 2 つの読み取り専用ロールと 2 つの操作ロールが含まれています。これらのロールは IdP を信頼して、アサーションでロールの名前を渡すことにより、選択したグループがロールにアクセスすることを認証および許可します。ワークロー

ドのアカウント 1 とアカウント 2 には、対応する読み取り専用ロールと運用ロールがあります。ワークロードアカウント 1 の場合、EmergencyAccess_RO ロールは緊急アクセスアカウントにある EmergencyAccess_Role1_RO ロールを信頼します。この表では、ワークロードアカウントの読み取り専用ロール、運用ロール、および対応する緊急アクセスロール間の類似の信頼パターンを示しています。

緊急事態に備えたタスク

緊急アクセス設定を準備するために、緊急事態が発生する前に次のタスクを実行するようお勧めします。

1. IdP でダイレクト IAM フェデレーションアプリケーションを設定します。詳細については、「Okta でダイレクト IAM フェデレーションアプリケーションの 1 回限りの設定を行う」を参照してください。
2. イベント中にアクセス可能な緊急アクセスアカウントに IdP 接続を作成します。
3. 上記のマッピング表で説明されているように、緊急アクセスアカウントに緊急アクセスロールを作成します。
4. 各ワークロードアカウントに、信頼ポリシーと権限ポリシーを含む一時的な運用ロールを作成します。
5. IdP に一時的な運用グループを作成します。グループ名は、一時的な運用ロールの名前によって異なります。
6. 直接 IAM フェデレーションをテストします。
7. IdP の IdP フェデレーションアプリケーションを無効にして、通常の使用を防止します。

緊急フェイルオーバープロセス

IAM Identity Center インスタンスが使用できず、AWS 管理コンソールへの緊急アクセスを提供する必要があると判断した場合は、以下のフェイルオーバープロセスをお勧めします。

1. IdP 管理者は IdP でダイレクト IAM フェデレーションアプリケーションを有効にします。
2. ユーザーは、E メールリクエスト、Slack チャネル、その他の通信手段など、既存のメカニズムを通じて一時的運用グループへのアクセスをリクエストします。
3. 緊急アクセスグループに追加したユーザーは IdP にサインインし、緊急アクセスアカウントを選択すると、ユーザーは緊急アクセスアカウントで使用するロールを選択します。これらのロールから、緊急アカウントロールと相互に信頼されている、対応するワークロードアカウントのロールを引き受けることができます。

通常の運用に戻る

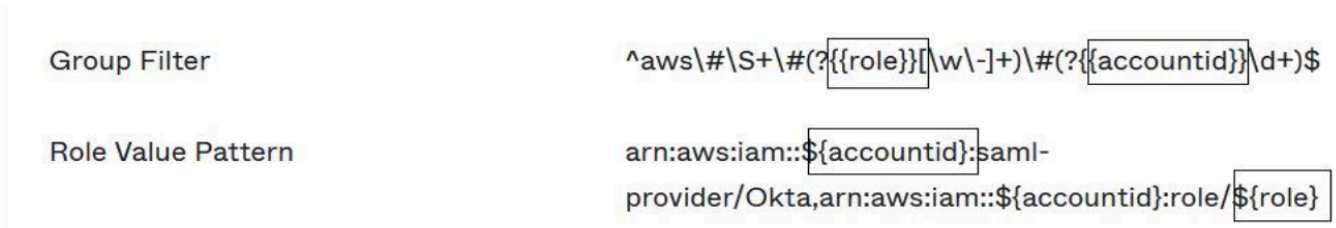
AWSHealth Dashboard をチェックして、IAM Identity Center サービスの状態がいつ回復したかを確認します。通常の運用に戻すには、次のステップを実行します。

1. IAM Identity Center サービスのステータスアイコンにサービスが正常であることが示されたら、IAM Identity Center にサインインします。
2. IAM Identity Center に正常にサインインできたら、IAM Identity Center が利用可能であることを緊急アクセスユーザーに伝えてください。これらのユーザーに、サインアウトし、AWS アクセスポータルを使用して IAM Identity Center にサインインし直すよう指示します。
3. すべての緊急アクセスユーザーがサインアウトしたら、IdP で IdP フェデレーションアプリケーションを無効にします。このタスクは勤務時間後に実行することをお勧めします。
4. IdP の緊急アクセスグループからすべてのユーザーを削除します。

緊急アクセスロールのインフラストラクチャはバックアップアクセスプランとしては残っていますが、現在は無効になっています。

Okta でダイレクト IAM フェデレーションアプリケーションの 1 回限りの設定を行う

1. 管理者アクセス権限を持つユーザーとしてご自身のOktaアカウントにサインインします。
2. Okta 管理コンソールの「アプリケーション」で、「アプリケーション」を選択します。
3. [アプリカタログを参照] を選択します。[AWS アカウントフェデレーション] を検索して選択します。それから[統合の追加] を選択します。
4. 「AWSアカウントフェデレーション用の SAML 2.0 の設定方法」の手順に従って、AWS で直接 IAM フェデレーションを設定します。
5. 「サインオンオプション」タブで「SAML 2.0」を選択し、「グループフィルター」と「ロール値パターン」の設定を入力します。ユーザーディレクトリのグループ名は、設定するフィルターによって異なります。



上の図では、role 変数は緊急アクセスアカウントの緊急運用のロール用です。例えば、(マッピング表で説明されているように) EmergencyAccess_Role1_RO ロールを AWS アカウント 123456789012 で作成し、グループフィルター設定が上の図のように構成されている場合、グループ名は aws#EmergencyAccess_Role1_RO#123456789012 になります。

6. ディレクトリ (Active Directory 内のディレクトリなど) に緊急アクセスグループを作成し、ディレクトリの名前 (例:aws#EmergencyAccess_Role1_RO#123456789012) を指定します。既存のプロビジョニングメカニズムを使用して、ユーザーをこのグループに割り当てます。

7. 緊急アクセスアカウントで、中断中に緊急アクセスの役割を引き受けるのに必要なアクセス許可を提供するカスタム信頼ポリシーを設定します。EmergencyAccess_Role1_RO ロールに添付されているカスタム 信頼ポリシー のステートメントの例を以下に示します。図については、緊急時のロール、アカウント、グループのマッピングを設計する方法 の図の緊急アカウントを参照してください。

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
         "Effect":"Allow",
         "Principal":{
            "Federated":"arn:aws:iam::123456789012:saml-provider/Okta"
         },
         "Action":[
            "sts:AssumeRoleWithSAML",
            "sts:SetSourceIdentity",
            "sts:TagSession"
         ],
         "Condition":{
            "StringEquals":{
               "SAML:aud":"https:~/~/signin.aws.amazon.com/saml"
            }
         }
      }
   ]
}
```

8. 以下は、EmergencyAccess_Role1_ROロールに適用されているアクセス 権限ポリシー のステートメントの例です。図については、緊急時のロール、アカウント、グループのマッピングを設計する方法 の図の緊急アカウントを参照してください。

```
{
    "Version": "2012-10-17",
    "Statement":[
      {
         "Effect":"Allow",
         "Action":"sts:AssumeRole",
         "Resource":[
            "arn:aws:iam::<account 1>:role/EmergencyAccess_RO",
            "arn:aws:iam::<account 2>:role/EmergencyAccess_RO"
         ]
      }
   ]
}
```

9. ワークロードアカウントで、カスタム信頼ポリシーを設定します。EmergencyAccess_RO ロールに添付されている 信頼ポリシー のステートメントの例を以下に示します。この例では、アカウント 123456789012 は緊急アクセスアカウントです。図については、緊急時のロール、アカウント、グループのマッピングを設計する方法の図の「ワークロードアカウント」を参照してください。

```
{
    "Version": "2012-10-17",
    "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "AWS":"arn:aws:iam::123456789012:root"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

> **Note**
>
> ほとんどの IdPs では、アプリケーション統合を必要なまで無効にしておくことができます。緊急アクセスが必要となるまで、IdP のダイレクト IAM フェデレーションアプリケーションを無効にしたままにしておくことをお勧めします。

のセキュリティ AWS IAM Identity Center

のクラウドセキュリティが最優先事項 AWS です。 AWS のお客様は、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャからメリットを得られます。

セキュリティは、 AWS とユーザーの間で共有される責任です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティとして説明しています。

- クラウドのセキュリティ — AWS クラウドで AWS サービスを実行するインフラストラクチャを保護する責任 AWS を担います。 AWS また、 は、お客様が安全に使用できるサービスも提供します。AWS コンプライアンスプログラムの一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。に適用されるコンプライアンスプログラムの詳細については AWS IAM Identity Center、「コンプライアンスAWS プログラムによる対象範囲内のサービス」を参照してください。
- クラウドのセキュリティ — お客様の責任は、使用する AWS サービスによって決まります。また、お客様は、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、IAM Identity Center が使用する際の責任共有モデルの適用法を理解するのに役立ちます。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するように IAM Identity Center を設定する方法について説明します。また、IAM Identity Center リソースのモニタリングや保護に役立つ他の AWS のサービスの使用方法についても説明します。

トピック

- IAM Identity Center の ID とアクセス管理
- IAM Identity Center コンソールと API 認証
- AWS STS IAM Identity Center の条件コンテキストキー
- IAM Identity Center でのロギングとモニタリング
- IAM Identity Center のコンプライアンス検証
- IAM Identity Center の障害への耐性
- IAM Identity Center でのインフラストラクチャのセキュリティ

IAM Identity Center の ID とアクセス管理

IAM Identity Center にアクセスするには AWS 、 がリクエストの認証に使用できる認証情報が必要です。これらの認証情報には、 AWS マネージドアプリケーションなどの AWS リソースにアクセスするためのアクセス許可が必要です。

AWS アクセスポータルへの認証は、IAM Identity Center に接続したディレクトリによって制御されます。ただし、 AWS アクセスポータル内からユーザーが利用できる に対する承認 AWS アカウントは、次の 2 つの要因によって決まります。

1. IAM Identity Center コンソール AWS アカウント でアクセス権が割り当てられているユーザー。詳細については、「へのシングルサインオンアクセス AWS アカウント」を参照してください。
2. それらの AWS アカウントに適切なアクセス権を付与するために、 IAM Identity Center コンソールでエンドユーザーにどのレベルのアクセス権限が付与されているか。詳細については、「アクセス許可セットの作成、管理と削除」を参照してください。

以下のセクションでは、管理者として IAM Identity Center コンソールへのアクセスを制御する方法、または IAM Identity Center コンソールから day-to-day タスクの管理アクセスを委任する方法について説明します。

- 認証
- アクセスコントロール

認証

IAM ID AWS を使用して にアクセスする方法について説明します。

アクセスコントロール

有効な認証情報があればリクエストを認証できますが、権限が付与されている場合を除き、IAM Identity Center リソースの作成やアクセスはできません。例えば、IAM Identity Center 接続先ディレクトリを作成するためのアクセス権限が必要です。

次のセクションでは、IAM Identity Center の権限を管理する方法について説明します。最初に概要のセクションを読むことをお勧めします。

- IAM Identity Center リソースへのアクセス権限の管理の概要

- IAM Identity Center の ID ベースのポリシーの例
- IAM Identity Center のサービスリンクロールの使用

IAM Identity Center リソースへのアクセス権限の管理の概要

すべての AWS リソースは によって所有され AWS アカウント、リソースを作成またはアクセスするためのアクセス許可はアクセス許可ポリシーによって管理されます。アクセスを提供するには、アカウント管理者は、IAM ID (つまり、ユーザー、グループ、ロール) に権限ポリシーを追加します。一部のサービス (AWS Lambdaなど) は、アクセス権限ポリシーをリソースに追加することができます。

> **Note**
>
> アカウント管理者 (または管理者ユーザー) は、管理者権限を持つユーザーです。詳細については、「IAM ユーザーガイド」の「IAM ベストプラクティス」を参照してください。

トピック

- IAM Identity Center リソースと運用
- リソース所有権について
- リソースへのアクセスの管理
- ポリシー要素の指定 : アクション、効果、リソース、プリンシパル
- ポリシーでの条件の指定

IAM Identity Center リソースと運用

IAM Identity Center で、主なリソースはアプリケーションのインスタンス、プロファイル、アクセス権限セットです。

リソース所有権について

リソース所有者は、リソースを作成した AWS アカウント です。つまり、リソース所有者は、リソースを作成するリクエスト AWS アカウント を認証するプリンシパルエンティティ (アカウント、ユーザー、または IAM ロール) の です。次の例は、この仕組みを示しています。

- がアプリケーションインスタンスやアクセス許可セットなどの IAM Identity Center リソース AWS アカウントのルートユーザー を作成する場合、 AWS アカウント はそのリソースの所有者です。

- AWS アカウントにユーザーを作成し、そのユーザーに IAM Identity Center リソースを作成するアクセス許可を付与すると、そのユーザーは IAM Identity Center リソースを作成できます。ただし、ユーザーが属する AWS アカウントがリソースを所有します。
- アカウントに IAM Identity Center リソースを作成するアクセス許可 AWS を持つ IAM ロールを作成すると、ロールを引き受けることのできるすべてのユーザーが IAM Identity Center リソースを作成できます。ロールが属する AWS アカウントは、IAM Identity Center リソースを所有しています。

リソースへのアクセスの管理

アクセス権限ポリシー では、誰が何にアクセスできるかを記述します。以下のセクションで、アクセス許可ポリシーを作成するために使用可能なオプションについて説明します。

> **Note**
>
> このセクションでは、IAM Identity Center のコンテキストでの IAM の使用について説明します。これは、IAM サービスに関する詳細情報を取得できません。IAM に関する詳細なドキュメントについては、「IAM ユーザーガイド」の「What is IAM?」(IAM とは？) を参照してください。IAM ポリシー構文の詳細と説明については、「IAM ユーザーガイド」の「AWS IAM ポリシーリファレンス」を参照してください。

IAM ID にアタッチされているポリシーは、ID ベース のポリシー (IAM ポリシー) と呼ばれます。リソースにアタッチされているポリシーは、リソースベース のポリシーと呼ばれます。IAM Identity Center では、ID ベースのポリシー (IAM ポリシー) のみがサポートされます。

トピック

- ID ベースのポリシー (IAM ポリシー)
- リソースベースのポリシー

ID ベースのポリシー (IAM ポリシー)

IAM ID にアクセス権限を追加できます。例えば、次のオペレーションを実行できます。

- のユーザーまたはグループにアクセス許可ポリシーをアタッチする AWS アカウント – アカウント管理者は、特定のユーザーに関連付けられたアクセス許可ポリシーを使用して、そのユーザーに新

しいアプリケーションなどの IAM Identity Center リソースを追加するアクセス許可を付与できます。

- アクセス権限ポリシーをロールにアタッチする (クロスアカウントの許可を付与) - ID ベースのアクセス権限ポリシーを IAM ロールにアタッチして、クロスアカウントの権限を付与することができます。

  IAM を使用したアクセス許可の委任の詳細については、「IAM ユーザーガイド」の「アクセス管理」を参照してください。

次のアクセス権限ポリシーは、`List` で始まるすべてのアクションを実行するためのアクセス権限をユーザーに付与します。これらのアクションは、アプリケーションインスタンスやアクセス権限セットなどの IAM Identity Center リソースに関する情報を表示します。`Resource` 要素内のワイルドカード文字 (*) は、アカウントによって所有されるすべての IAM Identity Center リソースに対してそれらのアクションが許可されることを示します。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"sso:List*",
         "Resource":"*"
      }
   ]
}
```

IAM Identity Center で ID ベースのポリシーを使用する場合の詳細については、 IAM Identity Center の ID ベースのポリシーの例 を参照してください。ユーザー、グループ、ロール、アクセス権限の詳細については、「IAM ユーザーガイド」の「ID (ユーザー、グループ、ロール)」を参照してください。

リソースベースのポリシー

Simple Storage Service (Amazon S3) などの他のサービスでは、リソースベースの許可ポリシーもサポートされています。例えば、ポリシーを S3 バケットにアタッチして、そのバケットに対するアクセス許可を管理できます。IAM Identity Center では、リソースベースのポリシーはサポートされていません。

ポリシー要素の指定 : アクション、効果、リソース、プリンシパル

IAM Identity Center のリソースごとに (「IAM Identity Center リソースと運用」参照)、このサービスは、一連の API オペレーションを定義します。こうした API 操作の権限を付与するために、IAM Identity Center はポリシーに特定できる一連のアクションを定義します。API オペレーションを実行する場合には、複数のアクションに対するアクセス許可が必要になることがあります。

以下は、基本的なポリシーの要素です。

- リソース – ポリシーで Amazon リソースネーム (ARN) を使用して、ポリシーを適用するリソースを識別します。
- アクション - アクションのキーワードを使用して、許可または拒否するリソースの操作を識別します。例えば、`sso:DescribePermissionsPolicies` 権限では、IAM アイデンティティセンター `DescribePermissionsPolicies` の操作を行うためのユーザー権限が与えられています。
- 効果 – ユーザーが特定のアクションを要求する際の効果を指定します。許可または拒否のいずれかになります。リソースへのアクセスを明示的に付与 (許可) していない場合、アクセスは暗黙的に拒否されます。また、明示的にリソースへのアクセスを拒否すると、別のポリシーによってアクセスが許可されている場合でも、ユーザーはそのリソースにアクセスできなくなります。
- プリンシパル - ID ベースのポリシー (IAM ポリシー) で、ポリシーがアタッチされているユーザーが黙示的なプリンシパルとなります。リソースベースのポリシーでは、権限 (リソースベースのポリシーにのみ適用) を受け取りたいユーザー、アカウント、サービス、またはその他のエンティティを指定します。IAM Identity Center では、リソースベースのポリシーはサポートされていません。

IAM ポリシーの構文と説明の詳細はこちら IAM ユーザーガイドの AWS IAM ポリシーリファレンス。

ポリシーでの条件の指定

アクセス権限を付与するとき、アクセスポリシー言語を使用して、ポリシーを有効にするために必要な条件を指定できます。例えば、特定の日付の後にのみ適用されるポリシーが必要になる場合があります。ポリシー言語での条件の指定の詳細については、「IAM ユーザーガイド」の「条件」を参照してください。

条件を表すには、あらかじめ定義された条件キーを使用します。IAM Identity Center に固有の条件キーはありません。ただし、必要に応じて使用できる AWS 条件キーがあります。 AWS キーの完全なリストについては、「IAM ユーザーガイド」の「利用可能なグローバル条件キー」を参照してください。

IAM Identity Center の ID ベースのポリシーの例

このトピックでは、IAM Identity Center を管理する権限をユーザーとロールに付与するために作成できる IAM ポリシーの例を紹介します。

> **Important**
>
> 初めに、IAM Identity Center のリソースへのアクセスを管理するための基本概念と使用可能なオプションについて説明する概要トピックをお読みになることをお勧めします。詳細については、「IAM Identity Center リソースへのアクセス権限の管理の概要」を参照してください。

このセクションでは、次のトピックを対象としています。

- カスタムポリシーの例
- IAM Identity Center コンソールの使用に必要な権限

カスタムポリシーの例

このセクションでは、カスタム IAM ポリシーを必要とする一般的なユースケースの例を示します。これらのポリシーの例は ID ベースのポリシーであり、プリンシパル要素を指定しません。これは、ID ベースのポリシーでは、権限を取得するプリンシパルを指定しないためです。代わりに、ポリシーをプリンシパルにアタッチします。IAM ロールに ID ベースの権限ポリシーをアタッチすると、ロールの信頼ポリシーで識別されたプリンシパルが許可を得ることになります。IAM で ID ベースのポリシーを作成し、ユーザー、グループ、ロールにアタッチできます。IAM Identity Center でアクセス権限セットを作成するときに、これらのポリシーを IAM Identity Center のユーザーに適用することもできます。

> **Note**
>
> お使いの環境用のポリシーを作成するときにこれらの例を使用し、これらのポリシーを本番環境に展開する前に、肯定的な (「アクセス許可」) テストケースと否定的な (「アクセス拒否」) テストケースの両方をテストしてください。IAM ポリシーシミュレーターの詳細については、「IAM ユーザーガイド」の「Testing IAM policies with the IAM policy simulator」(IAM Policy Simulator を使用した IAM ポリシーのテスト) を参照してください。

トピック

例 1: ユーザーに IAM Identity Center の表示を許可する

次のアクセス権限ポリシーは、ユーザーに読み取り権限を付与し、IAM Identity Center 内で設定されたすべての設定やディレクトリ情報を閲覧できるようにします。

> **Note**
>
> このポリシーは、例示のみを目的として提供されています。本番環境では、IAM Identity Center の `ViewOnlyAccess` AWS マネージドポリシーを使用することをお勧めします。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ds:DescribeDirectories",
                "ds:DescribeTrusts",
                "iam:ListPolicies",
                "organizations:DescribeOrganization",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:ListAccountsForParent",
                "organizations:ListOrganizationalUnitsForParent",
                "sso:ListManagedPoliciesInPermissionSet",
                "sso:ListPermissionSetsProvisionedToAccount",
                "sso:ListAccountAssignments",
                "sso:ListAccountsForProvisionedPermissionSet",
```

```
                "sso:ListPermissionSets",
                "sso:DescribePermissionSet",
                "sso:GetInlinePolicyForPermissionSet",
                "sso-directory:DescribeDirectory",
                "sso-directory:SearchUsers",
                "sso-directory:SearchGroups"
            ],
            "Resource": "*"
        }
    ]
}
```

例 2: IAM Identity Center AWS アカウント で へのアクセス許可をユーザーに管理することを許可する

以下のアクセス権限ポリシーでは、ユーザーが AWS アカウントアカウントのアクセス権限セットを作成、管理、デプロイできる許可を付与しています。

```
{
    "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**
>
> 、、および "Sid": "AccessToSSOProvisiondRoles"セクションにリストされている追加のアクセス許可は"Sid": "IAMListPermissions"、ユーザーが AWS Organizations 管理アカウントで割り当てを作成できるようにするためにのみ必要です。場合によっては、これらのセクションに iam:UpdateSAMLProvider を追加する必要もあります。

例 3: IAM Identity Center でのアプリケーション管理をユーザーに許可する

以下のアクセス権限ポリシーは、IAM Identity Center カタログ内から事前に統合された SaaS アプリケーションを含む IAM Identity Center のアプリケーションをユーザーが表示および設定できるようにするための許可を付与するものです。

> **Note**
>
> 以下のポリシー例で使用されている `sso:AssociateProfile` 操作は、ユーザーおよびグループのアプリケーションへの割り当てを管理するために必要です。また、ユーザーは既存のアクセス許可セット AWS アカウント を使用して、 にユーザーとグループを割り当てることもできます。ユーザーが IAM Identity Center 内で AWS アカウント アクセスを管理する必要があり、アクセス許可セットを管理するために必要なアクセス許可が必要な場合は、「」を参照してください例 2: IAM Identity Center AWS アカウント で へのアクセス許可をユーザーに管理することを許可する。

2020 年 10 月時点で、これらの運用の多くは AWS コンソールからのみ利用可能です。この例のポリシーには、リスト、取得、検索などの「読み取り」アクションが含まれており、この場合のコンソールエラーのないオペレーションに関連します。

```
{
    "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": "*"
        }
    ]
}
```

例 4: Identity Center ディレクトリのユーザーとグループの管理をユーザーに許可する

以下のアクセス権限ポリシーは、ユーザーが IAM Identity Center でユーザーとグループを作成、表示、修正、削除するための許可を付与します。

場合によっては、IAM Identity Center のユーザーやグループを直接変更することが制限されている場合もあります。例えば、アクティブディレクトリや、自動プロビジョニングが有効になっている外部の ID プロバイダーが ID ソースとして選択されている場合などです。

```
{
    "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": "*"
        }
    ]
}
```

IAM Identity Center コンソールの使用に必要な権限

ユーザーが IAM Identity Center コンソールをエラーなく使用するためには、追加の権限が必要です。これらの最小限必要な権限よりも制限された IAM ポリシーを作成している場合、そのポリシーを使用するユーザーに対してコンソールは意図したとおりには機能しません。以下の例では、IAM Identity Center コンソール内でエラーのない運用を行うために必要となる権限のセットを示しています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:DescribeAccountAssignmentCreationStatus",
                "sso:DescribeAccountAssignmentDeletionStatus",
                "sso:DescribePermissionSet",
                "sso:DescribePermissionSetProvisioningStatus",
```

```
                "sso:DescribePermissionsPolicies",
                "sso:DescribeRegisteredRegions",
                "sso:GetApplicationInstance",
                "sso:GetApplicationTemplate",
                "sso:GetInlinePolicyForPermissionSet",
                "sso:GetManagedApplicationInstance",
                "sso:GetMfaDeviceManagementForDirectory",
                "sso:GetPermissionSet",
                "sso:GetPermissionsPolicy",
                "sso:GetProfile",
                "sso:GetSharedSsoConfiguration",
                "sso:GetSsoConfiguration",
                "sso:GetSSOStatus",
                "sso:GetTrust",
                "sso:ListAccountAssignmentCreationStatus",
                "sso:ListAccountAssignmentDeletionStatus",
                "sso:ListAccountAssignments",
                "sso:ListAccountsForProvisionedPermissionSet",
                "sso:ListApplicationInstanceCertificates",
                "sso:ListApplicationInstances",
                "sso:ListApplications",
                "sso:ListApplicationTemplates",
                "sso:ListDirectoryAssociations",
                "sso:ListInstances",
                "sso:ListManagedPoliciesInPermissionSet",
                "sso:ListPermissionSetProvisioningStatus",
                "sso:ListPermissionSets",
                "sso:ListPermissionSetsProvisionedToAccount",
                "sso:ListProfileAssociations",
                "sso:ListProfiles",
                "sso:ListTagsForResource",
                "sso-directory:DescribeDirectory",
                "sso-directory:DescribeGroups",
                "sso-directory:DescribeUsers",
                "sso-directory:ListGroupsForUser",
                "sso-directory:ListMembersInGroup",
                "sso-directory:SearchGroups",
                "sso-directory:SearchUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS IAM Identity Center の マネージドポリシー

チームが必要とする権限のみを提供する IAM カスタマーマネージメントポリシーを作成するには、時間と専門知識が必要です。 AWS 管理ポリシーを使用すると、すぐに使用を開始できます。これらのポリシーは、一般的なユースケースをターゲット範囲に含めており、 AWS アカウントで利用できます。 AWS マネージドポリシーの詳細については、IAM ユーザーガイドの「AWS マネージドポリシー」を参照してください。

AWS サービスは、 AWS マネージドポリシーを維持および更新します。 AWS 管理ポリシーのアクセス許可は変更できません。サービスでは、新しい機能を利用できるようにするために、 AWS マネージドポリシーに権限が追加されることがあります。この種類の更新は、ポリシーがアタッチされている、すべてのアイデンティティ (ユーザー、グループおよびロール) に影響を与えます。新しい機能が立ち上げられた場合や、新しいオペレーションが使用可能になった場合に、各サービスが AWS マネージドポリシーを更新する可能性が最も高くなります。サービスは AWS マネージドポリシーからアクセス許可を削除しないため、ポリシーの更新によって既存のアクセス許可が破損することはありません。

さらに、 は、複数の サービスにまたがる職務機能の マネージドポリシー AWS をサポートします。例えば、 ReadOnlyAccess AWS 管理ポリシーは、すべての AWS サービスとリソースへの読み取り専用アクセスを提供します。サービスが新機能を起動すると、 は新しいオペレーションとリソースの読み取り専用アクセス許可 AWS を追加します。ジョブ機能ポリシーのリストと説明については、IAM ユーザーガイド の「AWS ジョブ機能のマネージドポリシー」を参照してください。

ユーザーセッションを一覧表示したり削除したりできる新しいアクションが、新しい名前スペース `identitystore-auth` で利用できるようになりました。この名前スペースのアクションに対する追加の権限は、このページで更新されます。カスタム IAM ポリシーを作成するときは、`identitystore-auth` の後に `*` を使用しないでください。これは、現在または将来名前スペースに存在するすべてのアクションに適用されるためです。

AWS マネージドポリシー： AWSSSOMasterAccountAdministrator

`AWSSSOMasterAccountAdministrator` ポリシーは、プリンシパルに必要な管理上のアクションを提供するものです。このポリシーは、 AWS IAM Identity Center 管理者のジョブロールを実行するプリンシパルを対象としています。時間の経過とともに、提供されるアクションのリストは、IAM Identity Center の既存の機能と管理者として必要なアクションに一致するように更新されます。

`AWSSSOMasterAccountAdministrator` ポリシーは IAM ID にアタッチできます。`AWSSSOMasterAccountAdministrator` ポリシーを ID にアタッチすると、管理 AWS IAM Identity Center アクセス許可が付与されます。このポリシーを持つプリンシパルは、 AWS

Organizations 管理アカウントとすべてのメンバーアカウント内の IAM Identity Center にアクセスできます。このプリンシパルは、IAM Identity Center インスタンス、ユーザー、アクセス権限セット、割り当てを作成する機能を含む、すべての IAM Identity Center の運用を完全に管理することができます。プリンシパルは、 AWS 組織メンバーアカウント全体でこれらの割り当てをインスタンス化し、 AWS Directory Service マネージドディレクトリと IAM Identity Center 間の接続を確立することもできます。新しい管理機能がリリースされると、アカウント管理者にはこれらの権限が自動的に付与されます。

アクセス権限のグループ化

このポリシーは、提供された一連の許可に基づくステートメントごとにグループ化されます。

- `AWSSSOMasterAccountAdministrator` – IAM Identity Center が `AWSServiceRoleforSSO` という名前の サービスロール を IAM Identity Center に渡すことを許可します。これにより、後でそのロールを引き受けて、代わりにアクションを実行できるようになります。これは、ユーザーやアプリケーションが IAM Identity Center を有効にするときに必要です。詳細については、「へのアクセスを管理する AWS アカウント」を参照してください。
- `AWSSSOMemberAccountAdministrator` – IAM Identity Center がマルチアカウント AWS 環境でアカウント管理者アクションを実行できるようにします。詳細については、「AWS 管理ポリシー： AWSSSOMemberAccountAdministrator」を参照してください。
- `AWSSSOManageDelegatedAdministrator` — IAM Identity Center が組織の委任管理者を登録および登録解除できるようにします。

このポリシーのアクセス許可を確認するには、「 マネージドポリシーリファレンスAWSSSOMasterAccountAdministrator」の「」を参照してください。 AWS

ポリシーに関する追加情報。

IAM Identity Center が初めて有効になると、IAM Identity Center サービスは AWS Organizations 管理アカウント (以前のマスターアカウント) にサービスにリンクされたロールを作成し、IAM Identity Center がアカウントのリソースを管理できるようにします。必要なアクションは `iam:CreateServiceLinkedRole` と `iam:PassRole` で、以下のスニペットに示されています。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "AWSSSOCreateSLR",
```

```
         "Effect": "Allow",
         "Action": "iam:CreateServiceLinkedRole",
         "Resource": "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
         "Condition": {
            "StringLike": {
               "iam:AWSServiceName": "sso.amazonaws.com"
            }
         }
      },
      {
         "Sid":"AWSSSOMasterAccountAdministrator",
         "Effect":"Allow",
         "Action":"iam:PassRole",
         "Resource":"arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
         "Condition":{
             "StringLike":{
               "iam:PassedToService":"sso.amazonaws.com"
             }
         }
      },
   ]
}
```

AWS 管理ポリシー： AWSSSOMemberAccountAdministrator

`AWSSSOMemberAccountAdministrator` ポリシーは、プリンシパルに必要な管理上のアクションを提供するものです。このポリシーは、IAM Identity Center 管理者のジョブのロールを遂行するプリンシパルを対象とします。時間の経過とともに、提供されるアクションのリストは、IAM Identity Center の既存の機能と管理者として必要なアクションに一致するように更新されます。

`AWSSSOMemberAccountAdministrator` ポリシーは IAM ID にアタッチできます。`AWSSSOMemberAccountAdministrator` ポリシーを ID にアタッチすると、管理 AWS IAM Identity Center アクセス許可が付与されます。このポリシーを持つプリンシパルは、 AWS Organizations 管理アカウントとすべてのメンバーアカウント内の IAM Identity Center にアクセスできます。このプリンシパルは、ユーザー、アクセス権限セット、および割り当てを作成する機能を含む、すべての IAM Identity Center の運用を完全に管理することができます。プリンシパルは、 AWS 組織メンバーアカウント全体でこれらの割り当てをインスタンス化し、 AWS Directory Service マネージドディレクトリと IAM Identity Center 間の接続を確立することもできます。新しい管理機能がリリースされると、アカウント管理者にはこれらの権限が自動的に付与されます。

このポリシーのアクセス許可を確認するには、「 マネージドポリシーリファレンスAWSSSOMemberAccountAdministrator」の「」を参照してください。 AWS

ポリシーに関する追加情報。

IAM Identity Center 管理者は、IAM Identity Center ディレクトリストア (sso-directory) でユーザー、グループ、パスワードを管理します。アカウント管理者ロールには、以下のアクションの権限が含まれます。

- `"sso:*"`
- `"sso-directory:*"`

IAM Identity Center 管理者は、毎日のタスクを実行するために、以下の AWS Directory Service アクションに対する限定的なアクセス許可が必要です。

- `"ds:DescribeTrusts"`
- `"ds:UnauthorizeApplication"`
- `"ds:DescribeDirectories"`
- `"ds:AuthorizeApplication"`
- `“ds:CreateAlias”`

これらの権限により、IAM Identity Center の管理者は、既存のディレクトリを特定し、アプリケーションを管理して、IAM Identity Center で使用できるように設定することができます。各アクションの詳細については、「AWS Directory Service API 権限：アクション、リソース、参照する条件」を参照してください。

IAM Identity Center は、IAM ポリシーを使用して、IAM Identity Center ユーザーにアクセス許可を付与します。IAM Identity Center 管理者は、アクセス権限セットを作成し、それにポリシーをアタッチします。IAM Identity Center 管理者は、作成または更新するアクセス権限セットで使用するポリシーを選択できるように、既存のポリシーを一覧表示するには以下の権限が必要です。安全で機能的な権限を設定するには、IAM Identity Center の管理者が IAM Access Analyzer ポリシー検証を実行する権限を持っている必要があります。

- `"iam:ListPolicies"`
- `"access-analyzer:ValidatePolicy"`

IAM Identity Center 管理者は、日常業務を実行するために、以下の AWS Organizations アクションへの制限付きアクセスが必要です。

- "organizations:EnableAWSServiceAccess"
- "organizations:ListRoots"
- "organizations:ListAccounts"
- "organizations:ListOrganizationalUnitsForParent"
- "organizations:ListAccountsForParent"
- "organizations:DescribeOrganization"
- "organizations:ListChildren"
- "organizations:DescribeAccount"
- "organizations:ListParents"
- "organizations:ListDelegatedAdministrators"
- "organizations:RegisterDelegatedAdministrator"
- "organizations:DeregisterDelegatedAdministrator"

これらの権限により、IAM Identity Center の管理者は、組織リソース (アカウント) を操作して、以下のような基本的な IAM Identity Center 管理タスクを行うことができます。

- 組織に属する管理アカウントの特定
- 組織に属するメンバーアカウントの識別
- アカウントの AWS サービスアクセスの有効化
- 代理管理者の設定と管理

IAM Identity Center での委任管理者の使用の詳細については、「委任された管理」を参照してください。これらのアクセス許可を で使用する方法の詳細については AWS Organizations、「 AWS Organizations を他の AWS のサービスで使用する」を参照してください。

AWS マネージドポリシー: AWSSSODirectoryAdministrator

`AWSSSODirectoryAdministrator` ポリシーは IAM ID にアタッチできます。

このポリシーは、IAM Identity Center のユーザーとグループに対する管理権限を付与します。このポリシーが適用されたプリンシパルは、IAM Identity Center のユーザーとグループを更新することができます。

このポリシーのアクセス許可を確認するには、「 マネージドポリシーリファレンスAWSSSODirectoryAdministrator」の「」を参照してください。 AWS

AWS 管理ポリシー: AWSSSOReadOnly

AWSSSOReadOnly ポリシーは IAM ID にアタッチできます。

このポリシーは、ユーザーが IAM Identity Center の情報を閲覧するための読み取り専用の権限を付与します。このポリシーが適用されたプリンシパルは、IAM Identity Center のユーザーやグループを直接表示できません。IAM Identity Center では、このポリシーが適用されたプリンシパルを更新できません。例えば、これらの権限を持つプリンシパルは、IAM Identity Center 設定を閲覧することはできますが、設定値を変更することはできません。

このポリシーのアクセス許可を確認するには、「 マネージドポリシーリファレンスAWSSSOReadOnly」の「」を参照してください。 AWS

AWS マネージドポリシー: AWSSSODirectoryReadOnly

AWSSSODirectoryReadOnly ポリシーは IAM ID にアタッチできます。

このポリシーは、ユーザーが IAM Identity Center のユーザーとグループを閲覧するための読み取り専用の権限を付与します。このポリシーが適用されたプリンシパルは、IAM Identity Center の割り当て、アクセス権限セット、アプリケーション、または設定を表示できません。IAM Identity Center では、このポリシーが適用されたプリンシパルを更新できません。例えば、これらの権限を持つプリンシパルは、IAM Identity Center ユーザーを表示できますが、ユーザー属性の変更や MFA デバイスの割り当てはできません。

このポリシーのアクセス許可を確認するには、「 マネージドポリシーリファレンスAWSSSODirectoryReadOnly」の「」を参照してください。 AWS

AWS 管理ポリシー: AWSIdentitySyncFullAccess

AWSIdentitySyncFullAccess ポリシーは IAM ID にアタッチできます。

このポリシーが適用されたプリンシパルには、同期プロファイルの作成と削除、同期プロファイルと同期ターゲットとの関連付けまたは更新、同期フィルターの作成、一覧表示、削除、同期の開始または停止を行う完全なアクセス権があります。

アクセス許可の詳細

このポリシーのアクセス許可を確認するには、「 マネージドポリシーリファレンスAWSIdentitySyncFullAccess」の「」を参照してください。 AWS

AWS 管理ポリシー： AWSIdentitySyncReadOnlyAccess

`AWSIdentitySyncReadOnlyAccess` ポリシーは IAM ID にアタッチできます。

このポリシーは、ユーザーが ID 同期プロファイル、フィルター、およびターゲット設定に関する情報を確認できるようにする読み取り専用の権限を付与します。このポリシーが適用されているプリンシパルは、同期設定を更新できません。例えば、これらのアクセス許可を持つプリンシパルは ID 同期設定を表示できますが、プロファイルやフィルターの値を変更することはできません。

このポリシーのアクセス許可を確認するには、「 マネージドポリシーリファレンスAWSIdentitySyncReadOnlyAccess」の「」を参照してください。 AWS

AWS 管理ポリシー: AWSSSOServiceRolePolicy

`AWSSSOServiceRolePolicy` ポリシーは IAM ID に適用できません。

このポリシーは、IAM Identity Center が の特定の へのシングルサインオンアクセス権を持つユーザーを委任して強制できるようにするサービスにリンクされたロールにアタッチ AWS アカウントされます AWS Organizations。IAM を有効にすると、サービスにリンクされたロールが組織 AWS アカウント 内のすべての に作成されます。また、IAM Identity Center では、その後組織に追加されるすべてのアカウントに、同じサービスにリンクしたロールが作成されます。このロールは、IAM Identity Center が顧客に代わって各アカウントのリソースにアクセスすることを可能にします。
各 で作成されるサービスにリンクされたロール AWS アカウント には、 という名前が付けられますAWSServiceRoleForSSO。詳細については、「IAM Identity Center のサービスリンクロールの使用」を参照してください。

AWS マネージドポリシー： AWSIAMIdentityCenterAllowListForIdentityContext

IAM Identity Center アイデンティティコンテキストを持つロールを
引き受けると、 AWS Security Token Service （ AWS STS) は自動的
に`AWSIAMIdentityCenterAllowListForIdentityContext`ポリシーをロールにアタッチします。

このポリシーは、IAM アイデンティティセンターID コンテキストで引き受けられるロールで信頼できる ID の伝播を使用する場合に許可されるアクションのリストを提供します。このコンテキストで呼び出される他のすべてのアクションはブロックされます。ID コンテキストは `ProvidedContext` として渡されます。

このポリシーのアクセス許可を確認するには、「 マネージドポリシーリファレンスAWSIAMIdentityCenterAllowListForIdentityContext」の「」を参照してください。 AWS

IAM Identity Center での AWS マネージドポリシーの更新

次の表は、IAM Identity Center の AWS マネージドポリシーの更新について、このサービスがこれらの変更の追跡を開始してからのものです。このページの変更に関する自動通知については、[IAM Identity Center ドキュメントの履歴] ページの RSS フィードを購読してください。

変更	説明	日付
AWSIAMIdentityCenterAllowListForIdentityContext	このポリシーには`elasticmapreduce:AddJobFlowSteps` 、Amazon EMR での信頼できる ID `elasticmapreduce:DescribeCluster` の伝播をサポートする `elasticmapreduce:CancelSteps` 、`elasticmapreduce:DescribeStep` 、、、および `elasticmapreduce:ListSteps` アクションが含まれるようになりました。	2024 年 5 月 17 日
AWSIAMIdentityCenterAllowListForIdentityContext	このポリシーには、`qapps:CreateQApp` 、、`qapps:PredictProblemStatementFromConversation` `qapps:PredictQAppFromProblemStatement` 、`qapps:CopyQApp` 、`qapps:GetQApp` 、`qapps:ListQApps` 、`qapps:UpdateQApp` `qapps:DeleteQApp` 、`qapps:AssociateQAppWithUser` 、、`qapps:Dis`	2024 年 4 月 30 日

変更	説明	日付
	associateQAppFromUser 、qapps:ImportDocumentToQApp 、qapps:ImportDocumentToQAppSession 、qapps:CreateLibraryItem 、qapps:GetLibraryItem 、、、、qapps:UpdateLibraryItem qapps:CreateLibraryItemReview qapps:ListLibraryItems 、、および qapps:StopQAppSession アクションが含まれqapps:CreateSubscriptionToken qapps:StartQAppSession 、これらのセッションをサポートする AWS マネージドアプリケーションのアイデンティティ対応コンソールセッションをサポートするようになりました。	

変更	説明	日付
AWSSSOMasterAccountAdministrator	このポリシーには、これらのセッションをサポートする AWS マネージドアプリケーションのアイデンティティ対応コンソールセッションをサポートする `signin:CreateTrustedIdentityPropagationApplicationForConsole` および `signin:ListTrustedIdentityPropagationApplicationsForConsole` アクションが含まれるようになりました。	2024 年 4 月 26 日
AWSSSOMemberAccountAdministrator	このポリシーには、これらのセッションをサポートする AWS マネージドアプリケーションのアイデンティティ対応コンソールセッションをサポートする `signin:CreateTrustedIdentityPropagationApplicationForConsole` および `signin:ListTrustedIdentityPropagationApplicationsForConsole` アクションが含まれるようになりました。	2024 年 4 月 26 日

変更	説明	日付
AWSSSOReadOnly	このポリシーには、これらのセッションをサポートする AWS マネージドアプリケーションの ID 対応コンソールセッションをサポートする `signin:ListTrustedIdentityPropagationApplicationsForConsole` アクションが含まれるようになりました。	2024 年 4 月 26 日
AWSIAMIdentityCenterAllowListForIdentityContext	このポリシーには、これらのセッションをサポートする AWS マネージドアプリケーションの ID 対応コンソールセッションをサポートする `qbusiness:PutFeedback` アクションが含まれるようになりました。	2024 年 4 月 26 日

変更	説明	日付
AWSIAMIdentityCenterAllowListForIdentityContext	このポリシーにはq:StartConversation 、これらのセッションをサポートするAWS マネージドアプリケーションのアイデンティティ対応コンソールセッションをサポートする q:SendMessage q:ListConversations q:GetConversation 、q:StartTroubleshootingResolutionExplanation 、、q:GetTroubleshootingResults 、q:StartTroubleshootingAnalysis 、、および q:UpdateTroubleshootingCommandResult アクションが含まれるようになりました。	2024 年 4 月 24 日
AWSIAMIdentityCenterAllowListForIdentityContext	このポリシーには、これらのセッションをサポートする AWS マネージドアプリケーションのアイデンティティ対応コンソールセッションをサポートするsts:SetContext アクションが含まれるようになりました。	2024 年 4 月 19 日

変更	説明	日付
AWSIAMIdentityCenterAllowListForIdentityContext	このポリシーにはqbusiness:Chat 、これらのセッションをサポートする AWS マネージドアプリケーションのアイデンティティ対応コンソールセッションをサポートする qbusiness:ChatSync qbusiness:ListConversations 、 qbusiness:ListMessages 、、、および qbusiness:DeleteConversation アクションが含まれるようになりました。	2024 年 4 月 11 日
AWSIAMIdentityCenterAllowListForIdentityContext	このポリシーには現在 s3:GetAccessGrantsInstanceForPrefix および s3:GetDataAccess アクションが含まれます。	2023 年 11 月 26 日
AWSIAMIdentityCenterAllowListForIdentityContext	このポリシーは、IAM アイデンティティセンターID コンテキストで引き受けられるロールで信頼できる ID の伝播を使用する場合に許可されるアクションのリストを提供します。	2023 年 11 月 15 日
AWSSSODirectoryReadOnly	このポリシーには、ユーザーがセッションを一覧表示して取得できるようにする新たな権限を付与された新しい名前スペース identitystore-auth が含まれました。	2023 年 2 月 21 日

変更	説明	日付
AWSSSOServiceRolePolicy	このポリシーにより、管理アカウントに対して UpdateSAMLProvider アクションを実行できるようになりました。	2022 年 10 月 20 日
AWSSSOMasterAccountAdministrator	このポリシーには、管理者がユーザーのセッションを一覧表示したり削除したりできるようにする新しい権限を持つ新しいネームスペース identitystore-auth が含まれるようになりました。	2022 年 10 月 20 日
AWSSSOMemberAccountAdministrator	このポリシーには、管理者がユーザーのセッションを一覧表示したり削除したりできるようにする新しい権限を持つ新しいネームスペース identitystore-auth が含まれるようになりました。	2022 年 10 月 20 日
AWSSSODirectoryAdministrator	このポリシーには、管理者がユーザーのセッションを一覧表示したり削除したりできるようにする新しい権限を持つ新しいネームスペース identitystore-auth が含まれるようになりました。	2022 年 10 月 20 日

変更	説明	日付
AWSSSOMasterAccountAdministrator	このポリシーには、ListDelegatedAdministrators で を呼び出すための新しいアクセス許可が含まれるようになりました AWS Organizations。このポリシーには、RegisterDelegatedAdministrator および DeregisterDelegatedAdministrator を呼び出すためのアクセス許可 AWSSSOManageDelegatedAdministrator を含むアクセス許可のサブセットも含まれるようになりました。	2022 年 8 月 16 日
AWSSSOMemberAccountAdministrator	このポリシーには、ListDelegatedAdministrators で を呼び出すための新しいアクセス許可が含まれるようになりました AWS Organizations。このポリシーには、RegisterDelegatedAdministrator および DeregisterDelegatedAdministrator を呼び出すためのアクセス許可 AWSSSOManageDelegatedAdministrator を含むアクセス許可のサブセットも含まれるようになりました。	2022 年 8 月 16 日

変更	説明	日付
AWSSSOReadOnly	このポリシーには、ListDelegatedAdministrators で を呼び出すための新しいアクセス許可が含まれるようになりましたAWS Organizations。	2022 年 8 月 11 日
AWSSSOServiceRolePolicy	このポリシーには、DeleteRolePermissionsBoundary 内の PutRolePermisionsBoundary を呼び出すための新しいアクセス許可が含まれるようになりました。	2022 年 7 月 14 日
AWSSSOServiceRolePolicy	このポリシーには、AWS Organizations内の ListAWSServiceAccessForOrganization and ListDelegatedAdministrators を呼び出すための新しいアクセス権が含まれました。	2022 年 5 月 11 日
AWSSSOMasterAccountAdministrator AWSSSOMemberAccountAdministrator AWSSSOReadOnly	プリンシパルが検証のためにポリシー チェックを使用できるようにする IAM Access Analyzer 権限を追加します。	2022 年 4 月 28 日

変更	説明	日付
AWSSSOMasterAccountAdministrator	このポリシーにより、IAM ID Center ID Store のすべてのサービスアクションが許可されるようになりました。 IAM ID センター ID Store サービスで使用できるアクションについては、IAM Identity Center Identity Store API Reference を参照してください。	2022 年 3 月 29 日
AWSSSOMemberAccountAdministrator	このポリシーにより、IAM ID Center ID Store のすべてのサービスアクションが許可されるようになりました。	2022 年 3 月 29 日
AWSSSODirectoryAdministrator	このポリシーにより、IAM ID Center ID Store のすべてのサービスアクションが許可されるようになりました。	2022 年 3 月 29 日
AWSSSODirectoryReadOnly	このポリシーは、IAM Identity Center Identity Store サービスの読み取りアクションへのアクセスを許可するようになりました。このアクセスは、IAM Identity Center Identity Store サービスからユーザーとグループの情報を取得するために必要です。	2022 年 3 月 29 日
AWSIdentitySyncFullAccess	このポリシーは、ID 同期許可への全アクセスを許可します。	2022 年 3 月 3 日

変更	説明	日付
AWSIdentitySyncReadOnlyAccess	このポリシーは、プリンシパルが ID 同期設定を閲覧するための読み取り専用の権限を付与します。	2022 年 3 月 3 日
AWSSSOReadOnly	このポリシーは、プリンシパルがすべての IAM Identity Center 構成設定を閲覧できる読み取り専用の権限を付与します。	2021 年 8 月 4 日
IAM Identity Center が変更の追跡を開始	IAM Identity Center が AWS マネージドポリシーの変更の追跡を開始しました。	2021 年 8 月 4 日

IAM Identity Center のサービスリンクロールの使用

AWS IAM Identity Center は AWS Identity and Access Management 、 (IAM) サービスにリンクされたロール を使用します。サービスリンクロールは、IAM Identity Center に直接リンクされた特殊なタイプの IAM ロールです。これは IAM Identity Center によって事前定義されており、サービスがユーザーに代わって他の AWS サービスを呼び出すために必要なすべてのアクセス許可が含まれています。詳細については、「サービスリンクロール」を参照してください。

サービスにリンクされたロールを使用すると、必要なアクセス許可を手動で追加する必要がないため、IAM Identity Center の設定が簡単になります。サービスリンクロールの許可は IAM Identity Center が定義し、特に定義されない限り、IAM Identity Center のみがそのロールを引き受けることができます。定義されたアクセス許可には、信頼ポリシーとアクセス権限ポリシーが含まれ、そのアクセス権限ポリシーを他の IAM エンティティに適用することはできません。

サービスにリンクされたロールをサポートする他のサービスについては、「IAM と連携するAWS サービス」を参照して、サービスにリンクされたロール 列が [はい]になっているサービスを見つけてください。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[はい] リンクを選択します。

IAM Identity Center のサービスリンクロールの権限

IAM Identity Center は、 という名前のサービスにリンクされたロールAWSServiceRoleForSSOを使用して、ユーザーに代わって IAM ロール、ポリシー、SAML IdP などの AWS リソースを管理するアクセス許可を IAM Identity Center に付与します。

AWSServiceRoleForSSO サービスにリンクされたロールは、次のサービスを信頼してロールを引き受けます。

- `IAM Identity Center`

AWSServiceRoleForSSO サービスにリンクされたロールのアクセス許可ポリシーにより、IAM Identity Center はパス「/aws-reserved/sso.amazonaws.com/”」と名前プレフィックス AWSReservedSSO「_」のロールで以下を完了できます。

- `iam:AttachRolePolicy`
- `iam:CreateRole`
- `iam:DeleteRole`
- `iam:DeleteRolePermissionsBoundary`
- `iam:DeleteRolePolicy`
- `iam:DetachRolePolicy`
- `iam:GetRole`
- `iam:ListRolePolicies`
- `iam:PutRolePolicy`
- `iam:PutRolePermissionsBoundary`
- `iam:ListAttachedRolePolicies`

AWSServiceRoleForSSO サービスにリンクされたロールのアクセス許可ポリシーにより、IAM Identity Center は、名前のプレフィックスがAWSSSO「_」の SAML プロバイダーで以下を完了できます。

- `iam:CreateSAMLProvider`
- `iam:GetSAMLProvider`
- `iam:UpdateSAMLProvider`
- `iam:DeleteSAMLProvider`

AWSServiceRoleForSSO サービスにリンクされたロールのアクセス許可ポリシーにより、IAM Identity Center はすべての組織で以下を完了できます。

- `organizations:DescribeAccount`
- `organizations:DescribeOrganization`
- `organizations:ListAccounts`
- `organizations:ListAWSServiceAccessForOrganization`
- `organizations:ListDelegatedAdministrators`

AWSServiceRoleForSSO サービスにリンクされたロールのアクセス許可ポリシーにより、IAM Identity Center はすべての IAM ロール (*) で以下を完了できます。

- `iam:listRoles`

AWSServiceRoleForSSO サービスにリンクされたロールのアクセス許可ポリシーにより、IAM Identity Center は「arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/AWSServiceRoleForSSO」で次のことを完了できます。

- `iam:GetServiceLinkedRoleDeletionStatus`
- `iam:DeleteServiceLinkedRole`

ロールのアクセス権限ポリシーは、リソースに対して以下のアクションを実行することを IAM Identity Center に許可します。

```
{
   "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":[
            "*"
         ]
```

```
        }
    ]
}
```

サービスリンクロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、アクセス許可を設定する必要があります。詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールのアクセス許可」を参照してください。

IAM Identity Center のサービスリンクロールの作成

サービスリンクロールを手動で作成する必要はありません。有効にすると、IAM Identity Center は AWS Organizations の組織内のすべてのアカウントにサービスにリンクされたロールを作成します。また、IAM Identity Center では、その後組織に追加されるすべてのアカウントに、同じサービスにリンクしたロールが作成されます。このロールは、IAM Identity Center が顧客に代わって各アカウントのリソースにアクセスすることを可能にします。

メモ

- AWS Organizations 管理アカウントにサインインしている場合、サービスにリンクされたロールではなく、現在サインインしているロールが使用されます。これにより、権限の昇格を防ぐことができます。
- IAM Identity Center が AWS Organizations 管理アカウントで IAM オペレーションを実行すると、すべてのオペレーションは IAM プリンシパルの認証情報を使用して行われます。これにより、 のログイン CloudTrail により、管理アカウントですべての権限変更を行ったユーザーを可視化できます。

Important

サービスにリンクされたロールのサポートが開始された 2017 年 12 月 7 日より前に IAM Identity Center サービスを使用していた場合、IAM Identity Center はアカウントに AWSServiceRoleForSSO ロールを作成しました。詳細については、「IAM アカウントに新しいロールが表示される」を参照してください。

このサービスにリンクされたロールを削除した後で再度作成する必要が生じた場合は、同じ方法でアカウントにロールを再作成できます。

IAM Identity Center のサービスリンクロールの編集

IAM Identity Center では、 AWSServiceRoleForSSO サービスにリンクされたロールを編集することはできません。サービスリンクロールを作成した後は、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロールの説明の編集はできます。詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールの編集」を参照してください。

IAM Identity Center のサービスリンクロールの削除

AWSServiceRoleForSSO ロールを手動で削除する必要はありません。 AWS アカウント が AWS 組織から削除されると、IAM Identity Center は自動的にリソースをクリーンアップし、その からサービスにリンクされたロールを削除します AWS アカウント。

サービスにリンクされたロールは、IAM コンソール、IAM CLI、または IAM API を使用して手動で削除することもできます。そのためにはまず、サービスリンクロールのリソースをクリーンアップする必要があります。その後で、手動で削除できます。

> **Note**
>
> リソースを削除しようとしたときに IAM Identity Center サービスがロールを使用している場合は、削除が失敗する可能性があります。失敗した場合は、数分待ってから操作を再試行してください。

によって使用されている IAM Identity Center リソースを削除するには AWSServiceRoleForSSO

1. AWS アカウントへのアクセス権を持つすべてのユーザーとグループの ユーザーとグループのアクセス権限を削除。
2. AWS アカウントに関連付けられている アクセス権限セットを削除する。

サービスにリンクされたロールを IAM で手動削除するには

IAM コンソール、IAM CLI、または IAM API を使用して、サービスにリンクされたロールを削除します AWSServiceRoleForSSO。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの削除」を参照してください。

IAM Identity Center コンソールと API 認証

既存の IAM アイデンティティセンターコンソール API は二重認証をサポートしているため、新しい API が利用可能になっても既存の API オペレーションを引き続き使用できます。2023 年 11 月 15 日および 2020 年 10 月 15 日より前に作成された IAM アイデンティティセンターの既存のインスタンスがある場合は、次の表を使用して、どの API オペレーションがそれらの日付以降にリリースされた新しい API オペレーションにマップされているかを判断できます。

トピック

2023 年 11 月以降の API アクション

2023 年 11 月 15 日より前に作成された IAM アイデンティティセンターのインスタンスは、いずれかのアクションに対して明示的な拒否がない限り、新旧両方の API アクションを受け入れます。2023 年 11 月 15 日以降に作成されたインスタンスは、IAM アイデンティティセンターコンソールの認証に 新しい API アクションを使用します。

2023 年 11 月 15 日以前に使用されたコンソールオペレーション名	2023 年 11 月 15 日以降に使用された API アクション
AssociateProfile	CreateApplicationAssignment
CreateManagedApplicationInstance | CreateApplicationInstance	CreateApplication
CreateManagedApplicationInstance	PutApplicationAuthenticationMethod
DeleteApplicationInstance | DeleteManagedApplicationInstance	DeleteApplication
DeleteSSO	DeleteInstance
DisassociateProfile	DeleteApplicationAssignment
GetApplicationTemplate	DescribeApplicationProvider

2023 年 11 月 15 日以前に使用されたコンソールオペレーション名	2023 年 11 月 15 日以降に使用された API アクション
GetManagedApplicationInstance	DescribeApplication
GetSharedSsoConfiguration	DescribeInstance
ListApplicationInstances	ListApplications
ListApplicationTemplates	ListApplicationProviders
ListDirectoryAssociations	DescribeInstance
ListProfileAssociations	ListApplicationAssignments
UpdateApplicationInstanceDisplayData | UpdateApplicationInstanceStatus | UpdateManagedApplicationInstanceStatus	UpdateApplication

2020 年 10 月以降の API アクション

2020 年 10 月 15 日以前に作成された IAM アイデンティティセンターのインスタンスは、いずれかのアクションに明示的な拒否がない限り、新旧両方の API アクションを受け入れます。2020 年 10 月 15 日以降に作成されたインスタンスは、IAM アイデンティティセンターコンソールでの認証に新しい API アクションを使用します。

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
AssociateProfile	AssociateProfile	CreateAccountAssignment
AttachManagedPolicy	PutPermissionsPolicy	AttachManagedPolicyToPermissionSet
CreatePermissionSet	CreatePermissionSet	CreatePermissionSet
DeleteApplicationInstanceForAWsAccount	DeleteApplicationInstance | DeleteTrust	DeleteAccountAssignment

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
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
ListPermissionSets	ListPermissionSets	ListPermissionSets
ListProfileAssociations	ListProfileAssociations	ListAccountAssignments

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
ProvisionApplicationInstanceForAWSAccount	GetApplicationInstance | CreateApplicationInstance	CreateAccountAssignment
ProvisionApplicationProfileForAWSAccountInstance	GetProfile | CreateProfile | UpdateProfile	CreateAccountAssignment
ProvisionSAMLProvider	GetTrust | CreateTrust | UpdateTrust	CreateAccountAssignment
PutPermissionsPolicy	PutPermissionsPolicy	PutInlinePolicyToPermissionSet
UpdatePermissionSet	UpdatePermissionSet	UpdatePermissionSet

AWS STS IAM Identity Center の条件コンテキストキー

プリンシパルが にリクエストを行うと AWS、 はリクエスト情報をリクエストコンテキスト に AWS 収集し、リクエストの評価と承認に使用されます。JSON ポリシーの `Condition` 要素を使用して、リクエストコンテキストのキーを、ポリシーで指定したキー値と比較できます。リクエスト情報は、リクエストを行うプリンシパル、リソース、リクエストが行われたリクエスト、リクエスト自体に関するメタデータなど、さまざまなソースから提供されます。サービス固有の条件キーは、個々の AWS サービスで使用するように定義されます。

IAM Identity Center には、 AWS マネージドアプリケーションとサードパーティーアプリケーションが IAM Identity Center で定義される条件キーの値を追加できるようにする AWS STS コンテキストプロバイダーが含まれています。これらのキーは IAM ロール に含まれています。キー値は、アプリケーションがトークンを に渡すときに設定されます AWS STS。アプリケーションは、次のいずれか AWS STS の方法で に渡されるトークンを取得します。

- IAM Identity Center での認証中。
- 信頼できるトークン発行者とトークン交換して、信頼できる ID を伝播した後。この場合、アプリケーションは信頼できるトークン発行者からトークンを取得し、そのトークンを IAM Identity Center からのトークンと交換します。

これらのキーは通常、信頼できる ID の伝播と統合するアプリケーションで使用されます。場合によっては、キー値が存在するときに、作成した IAM ポリシーでこれらのキーを使用してアクセス許可を許可または拒否できます。

例えば、 の値に基づいてリソースへの条件付きアクセスを提供することができますUserId。この値は、ロールを使用している IAM Identity Center ユーザーを示します。この例は、 の使用に似ていますSourceId。ただしSourceId、 とは異なり、 の値は ID ストアから特定の検証済みユーザーUserId を表します。この値は、アプリケーションが取得して に渡すトークンに存在しますAWS STS。任意の値を含めることができる汎用文字列ではありません。

トピック

- ID ストア：UserId
- ID ストア：IdentityStoreArn
- アイデンティティセンター：ApplicationArn
- アイデンティティセンター：CredentialId
- アイデンティティセンター：InstanceArn

ID ストア：UserId

このコンテキストキーは、IAM Identity Center UserId によって発行されたコンテキストアサーションの対象となる IAM Identity Center ユーザーの です。コンテキストアサーションは に渡されますAWS STS。このキーを使用して、リクエストが行われた IAM Identity Center UserId ユーザーのを、ポリシーで指定したユーザーの識別子で比較できます。

- 可用性 — このキーは、IAM Identity Center によって発行されたコンテキストアサーションが設定された後、 AWS CLI または AWS STS AssumeRole API オペレーションのコマンドを使用して AWS STS assume-roleロールが引き受けられたときに、リクエストコンテキストに含まれます。
- データ型 - 文字列
- 値タイプ — 単一値

ID ストア：IdentityStoreArn

このコンテキストキーは、コンテキストアサーションを発行した IAM Identity Center のインスタンスにアタッチされている ID ストアの ARN です。また、 の属性を検索できる ID ストアでもありま

すidentitystore:UserID。このキーをポリシーで使用して、 が期待される ID ストア ARN からのidentitystore:UserIDものであるかどうかを判断できます。

- 可用性 — このキーは、IAM Identity Center によって発行されたコンテキストアサーションが設定された後、 AWS CLI または AWS STS AssumeRole API オペレーションのコマンド AWS STS assume-roleを使用してロールが引き受けられたときに、リクエストコンテキストに含まれます。
- データ型 – Arn 、文字列
- 値タイプ — 単一値

アイデンティティセンター：ApplicationArn

このコンテキストキーは、IAM Identity Center がコンテキストアサーションを発行したアプリケーションの ARN です。このキーをポリシーで使用して、 が想定されたアプリケーションからのidentitycenter:ApplicationArnものであるかどうかを判断できます。このキーを使用すると、IAM ロールが予期しないアプリケーションからアクセスされるのを防ぐことができます。

- 可用性 — このキーは API AWS STS AssumeRoleオペレーションのリクエストコンテキストに含まれます。リクエストコンテキストには、IAM Identity Center によって発行されたコンテキストアサーションが含まれます。
- データ型 – Arn 、文字列
- 値タイプ — 単一値

アイデンティティセンター：CredentialId

このコンテキストキーは、アイデンティティが強化されたロール認証情報のランダム ID であり、ログ記録にのみ使用されます。このキー値は予測できないため、ポリシーのコンテキストアサーションには使用しないことをお勧めします。

- 可用性 — このキーは API AWS STS AssumeRoleオペレーションのリクエストコンテキストに含まれます。リクエストコンテキストには、IAM Identity Center によって発行されたコンテキストアサーションが含まれます。
- データ型 - 文字列
- 値タイプ — 単一値

アイデンティティセンター：InstanceArn

このコンテキストキーは、 のコンテキストアサーションを発行した IAM Identity Center のインスタンスの ARN ですidentitystore:UserID。このキーを使用して、 identitystore:UserIDおよび コンテキストアサーションが、予想される IAM Identity Center インスタンス ARN から送信されたかどうかを判断できます。

- 可用性 — このキーは API AWS STS AssumeRoleオペレーションのリクエストコンテキストに含まれます。リクエストコンテキストには、IAM Identity Center によって発行されたコンテキストアサーションが含まれます。
- データ型 – Arn 、文字列
- 値タイプ — 単一値

IAM Identity Center でのロギングとモニタリング

ベストプラクティスとして、変更がログに記録されることを確実にするために組織を監視する必要があります。これにより、予期しない変更を調査でき、不要な変更をロールバックできます。 AWS IAM Identity Center は現在、組織とその内部で発生するアクティビティのモニタリングに役立つ 2 つの AWS サービスをサポートしています。

トピック

- を使用した IAM Identity Center API コールのログ記録 AWS CloudTrail
- Amazon EventBridge
- AD 同期エラーと設定可能な AD 同期エラーのログ記録

を使用した IAM Identity Center API コールのログ記録 AWS CloudTrail

AWS IAM Identity Center は AWS CloudTrail、IAM Identity Center のユーザー、ロール、またはサービスによって実行されたアクションを記録する AWS サービスである と統合されています。は、IAM Identity Center の API コールをイベントとして CloudTrail キャプチャします。キャプチャされた呼び出しには、IAM Identity Center コンソールからの呼び出しと、IAM Identity Center の API 運用へのコードの呼び出しが含まれます。証跡を作成する場合は、IAM Identity Center の CloudTrail イベントなど、Amazon S3 バケットへのイベントの継続的な配信を有効にすることができます。証跡を設定しない場合でも、 CloudTrail コンソールのイベント履歴 で最新のイベントを表示できます。で収集された情報を使用して CloudTrail、IAM Identity Center に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

の詳細については CloudTrail、「AWS CloudTrail ユーザーガイド」を参照してください。

トピック

- の IAM Identity Center 情報 CloudTrail
- IAM Identity Center のログファイルエントリーの概要
- IAM Identity Center サインインイベントの概要

の IAM Identity Center 情報 CloudTrail

CloudTrail アカウントを作成する AWS アカウント と、 で が有効になります。IAM Identity Center でアクティビティが発生すると、そのアクティビティは CloudTrail イベント履歴 の他の AWS サービスイベントとともにイベントに記録されます。 で最近のイベントを表示、検索、ダウンロードできます AWS アカウント。詳細については、「イベント履歴 を含む CloudTrail イベントの表示」を参照してください。

IAM Identity Center のイベントなど AWS アカウント、 のイベントの継続的な記録については、証跡を作成します。証跡により CloudTrail 、 はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成すると、すべての AWS リージョンに証跡が適用されます。証跡は、 AWS パーティション内のすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、 CloudTrail ログで収集されたイベントデータをより詳細に分析し、それに基づいて行動するように他の AWS サービスを設定できます。詳細については、次を参照してください:

- 「証跡作成の概要」
- CloudTrail がサポートするサービスと統合
- の Amazon SNS 通知の設定 CloudTrail
- 複数のリージョンからの CloudTrail ログファイルの受信と複数のアカウントからのログファイルの受信 CloudTrail

で CloudTrail ログ記録が有効になっている場合 AWS アカウント、IAM Identity Center アクションに対して行われた API コールはログファイルで追跡されます。IAM Identity Center レコードは、他の AWS サービスレコードと一緒にログファイルに書き込まれます。 は、期間とファイルサイズに基づいて、新しいファイルを作成して書き込むタイミング CloudTrail を決定します。

以下の IAM Identity Center CloudTrail オペレーションがサポートされています。

コンソール API オペレーション	公開 API オペレーション
AssociateDirectory	AttachManagedPolicyToPermissionSet
AssociateProfile	CreateAccountAssignment
BatchDeleteSession	CreateInstanceAccessControlAttributeConfiguration
BatchGetSession	CreatePermissionSet
CreateApplicationInstance	DeleteAccountAssignment
CreateApplicationInstanceCertificate	DeleteInlinePolicyFromPermissionSet
CreatePermissionSet	DeleteInstanceAccessControlAttributeConfiguration
CreateProfile	DeletePermissionSet
DeleteApplicationInstance	DescribeAccountAssignmentCreationStatus
DeleteApplicationInstanceCertificate	DescribeAccountAssignmentDeletionStatus
DeletePermissionsPolicy	DescribeInstanceAccessControlAttributeConfiguration
DeletePermissionSet	DescribePermissionSet
DeleteProfile	DescribePermissionSetProvisioningStatus
DescribePermissionsPolicies	DetachManagedPolicyFromPermissionSet
DisassociateDirectory	GetInlinePolicyForPermissionSet

コンソール API オペレーション	公開 API オペレーション
DisassociateProfile	ListAccountAssignmentCreationStatus
GetApplicationInstance	ListAccountAssignmentDeletionStatus
GetApplicationTemplate	ListAccountAssignments
GetMfaDeviceManagementForDirectory	ListAccountsForProvisionedPermissionSet
GetPermissionSet	ListInstances
GetSSOStatus	ListManagedPoliciesInPermissionSet
ImportApplicationInstanceServiceProviderMetadata	ListPermissionSetProvisioningStatus
ListApplicationInstances	ListPermissionSets
ListApplicationInstanceCertificates	ListPermissionSetsProvisionedToAccount
ListApplicationTemplates	ListTagsForResource
ListDirectoryAssociations	ProvisionPermissionSet
ListPermissionSets	PutInlinePolicyToPermissionSet
ListProfileAssociations	TagResource
ListProfiles	UntagResource
ListSessions	UpdateInstanceAccessControlAttributeConfiguration

コンソール API オペレーション	公開 API オペレーション
PutMfaDeviceManagementForDirectory	UpdatePermissionSet
PutPermissionsPolicy	
StartSSO	
UpdateApplicationInstanceActiveCertificate	
UpdateApplicationInstanceDisplayData	
UpdateApplicationInstanceServiceProviderConfiguration	
UpdateApplicationInstanceStatus	
UpdateApplicationInstanceResponseConfiguration	
UpdateApplicationInstanceResponseSchemaConfiguration	
UpdateApplicationInstanceSecurityConfiguration	
UpdateDirectoryAssociation	
UpdateProfile	

IAM Identity Center のパブリック API 運用の詳細については、IAM Identity Center API Reference Guide を参照してください。

次の IAM Identity Center Identity Store CloudTrail オペレーションがサポートされています。

- AddMemberToGroup
- CompleteVirtualMfaDeviceRegistration

- CompleteWebAuthnDeviceRegistration
- CreateAlias
- CreateExternalIdPConfigurationForDirectory
- CreateGroup
- CreateUser
- DeleteExternalIdPConfigurationForDirectory
- DeleteGroup
- DeleteMfaDeviceForUser
- DeleteUser
- DescribeDirectory
- DescribeGroups
- DescribeUsers
- DisableExternalIdPConfigurationForDirectory
- DisableUser
- EnableExternalIdPConfigurationForDirectory
- EnableUser
- GetAWSSPConfigurationForDirectory
- ListExternalIdPConfigurationsForDirectory
- ListGroupsForUser
- ListMembersInGroup
- ListMfaDevicesForUser
- PutMfaDeviceManagementForDirectory
- RemoveMemberFromGroup
- SearchGroups
- SearchUsers
- StartVirtualMfaDeviceRegistration
- StartWebAuthnDeviceRegistration
- UpdateExternalIdPConfigurationForDirectory
- UpdateGroup

- UpdateMfaDeviceForUser
- UpdatePassword
- UpdateUser
- VerifyEmail

次の IAM Identity Center OIDC CloudTrail アクションがサポートされています。

- CreateToken
- RegisterClient
- StartDeviceAuthorization

以下の IAM Identity Center Portal CloudTrail アクションがサポートされています。

- Authenticate
- Federate
- ListApplications
- ListProfilesForApplication
- ListAccounts
- ListAccountRoles
- GetRoleCredentials
- Logout

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます:

- リクエストがルートユーザーまたは AWS Identity and Access Management (IAM) ユーザーの認証情報を使用して行われたかどうか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが別の AWS サービスによって行われたかどうか。

詳細については、CloudTrail userIdentity 要素」を参照してください。

IAM Identity Center のログファイルエントリーの概要

証跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信できるようにする設定です。 CloudTrail ログファイルには 1 つ以上のログエントリが含まれます。イベントは任意のソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどに関する情報が含まれます。 CloudTrail ログファイルはパブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

次の例は、IAM Identity Center コンソールで発生した管理者 (samadams@example.com) の CloudTrail ログエントリを示しています。


```
{
   "Records":[
      {
         "eventVersion":"1.05",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDAJAIENLMexample",
            "arn":"arn:aws:iam::08966example:user/samadams",
            "accountId":"08966example",
            "accessKeyId":"AKIAIIJM2K4example",
            "userName":"samadams"
         },
         "eventTime":"2017-11-29T22:39:43Z",
         "eventSource":"sso.amazonaws.com",
         "eventName":"DescribePermissionsPolicies",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"203.0.113.0",
         "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
         "requestParameters":{
            "permissionSetId":"ps-79a0dde74b95ed05"
         },
         "responseElements":null,
         "requestID":"319ac6a1-d556-11e7-a34f-69a333106015",
         "eventID":"a93a952b-13dd-4ae5-a156-d3ad6220b071",
         "readOnly":true,
         "resources":[

         ],
         "eventType":"AwsApiCall",
         "recipientAccountId":"08966example"
      }
```

```
   ]
}
```

次の例は、 AWS アクセスポータルで実行されたエンドユーザー (bobsmith@example.com) アクションの CloudTrail ログエントリを示しています。

```
{
   "Records":[
      {
         "eventVersion":"1.05",
         "userIdentity":{
            "type":"Unknown",
            "principalId":"example.com//
S-1-5-21-1122334455-3652759393-4233131409-1126",
            "accountId":"08966example",
            "userName":"bobsmith@example.com"
         },
         "eventTime":"2017-11-29T18:48:28Z",
         "eventSource":"sso.amazonaws.com",
         "eventName":"ListApplications",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"203.0.113.0",
         "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
         "requestParameters":null,
         "responseElements":null,
         "requestID":"de6c0435-ce4b-49c7-9bcc-bc5ed631ce04",
         "eventID":"e6e1f3df-9528-4c6d-a877-6b2b895d1f91",
         "eventType":"AwsApiCall",
         "recipientAccountId":"08966example"
      }
   ]
}
```

次の例は、IAM Identity Center OIDC で実行されたエンドユーザー (bobsmith@example.com) アクションの CloudTrail ログエントリを示しています。

```
{
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "Unknown",
        "principalId": "example.com//S-1-5-21-1122334455-3652759393-4233131409-1126",
```

```
        "accountId": "08966example",
        "userName": "bobsmith@example.com"
      },
      "eventTime": "2020-06-16T01:31:15Z",
      "eventSource": "sso.amazonaws.com",
      "eventName": "CreateToken",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "203.0.113.0",
      "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
      "requestParameters": {
        "clientId": "clientid1234example",
        "clientSecret": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "grantType": "urn:ietf:params:oauth:grant-type:device_code",
        "deviceCode": "devicecode1234example"
      },
      "responseElements": {
        "accessToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "tokenType": "Bearer",
        "expiresIn": 28800,
        "refreshToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "idToken": "HIDDEN_DUE_TO_SECURITY_REASONS"
      },
      "eventID": "09a6e1a9-50e5-45c0-9f08-e6ef5089b262",
      "readOnly": false,
      "resources": [
        {
          "accountId": "08966example",
          "type": "IdentityStoreId",
          "ARN": "d-1234example"
        }
      ],
      "eventType": "AwsApiCall",
      "recipientAccountId": "08966example"
}
```


IAM Identity Center サインインイベントの概要

AWS CloudTrail は、すべての AWS IAM Identity Center ID ソースのサインインイベントの成功と失敗を記録します。ネイティブ SSO および Active Directory (AD Connector および AWS Managed Microsoft AD) ソース ID には、ユーザーが特定の認証情報のチャレンジまたは要素を解決するように求められるたびにキャプチャされる追加のサインインイベントと、その特定の認証情報検証リクエス

トのステータスが含まれます。必要な認証情報のチャレンジをすべて完了したユーザーだけがサインインを許可され、UserAuthentication イベントが記録されます。

次の表は、IAM Identity Center の各サインイン CloudTrail イベント名、その目的、およびさまざまな ID ソースへの適用性を示しています。

イベント名	イベントの目的	ID ソースの適用性
CredentialChallenge	IAM Identity Center がユーザーに特定の認証課題の解決を要求したことを通知するために使用され、要求されている CredentialType を指定します (例として、PASSWORD または TOTP)。	ネイティブ IAM Identity Center ユーザー、AD Connector、および AWS Managed Microsoft AD
CredentialVerification	ユーザーが特定の CredentialChallenge リクエストの解決を試みたことを通知するために使用され、その認証情報が成功したか失敗したかを指定します。	ネイティブ IAM Identity Center ユーザー、AD Connector、および AWS Managed Microsoft AD
UserAuthentication	要求されたすべての認証要件をユーザーが正常に完了し、正常にサインインしたことを通知するために使用されます。ユーザーが必要な認証情報のチャレンジを正常に完了できなかった場合、*UserAuthentication* イベントはログに記録されません。	すべての ID ソース

次の表は、特定のサインインイベントに含まれるその他の有用な CloudTrail イベントデータフィールドをまとめたものです。

イベント名	イベントの目的	サインインイベントの適用性	値の例
AuthWorkflowID	サインインシーケンス全体で発生するすべてのイベントを相関させるために使用されます。各ユーザーのサインインに対して、IAM Identity Center は複数のイベントを発行することができます。	CredentialChallenge , CredentialVerification , UserAuthentication	AuthWorkflow「ID」：「9de74b32-8362-4a01-a524-de21df59fd83」
CredentialType	チャレンジされた認証またはファクターを指定するために使用されます。UserAuthentication イベントには、ユーザーのサインインーケンスで正常に検証された CredentialType 値がすべて含まれます。	CredentialChallenge , CredentialVerification , UserAuthentication	CredentialType「：」またはCredentialType「」：「PASSWORD,TOTP」(使用できる値には、PASSWORD, TOTP, WEBAUTHN, EXTERNAL_IDP, RESYNC_TOTP などがあります)
DeviceEnrollmentRequired	サインイン時に MFA デバイスの登録が要求され、ユーザーがその要求を正常に完了したことを示すために使用されます。	UserAuthentication	DeviceEnrollmentRequired「」：「true」
LoginTo	サインインに成功した後のリダイレクト	UserAuthentication	LoginTo「」:https://mydirectory.awsapps.com/start/....."

イベント名	イベントの目的	サインインイベントの適用性	値の例
	先を指定するために使用します。		

IAM Identity Center サインインシナリオのイベント例

次の例は、さまざまなサインインシナリオで想定される一連の CloudTrail イベントを示しています。

トピック

- パスワードのみを使用した認証での正常なサインイン
- 外部の ID プロバイダーで認証した場合のサインインの成功
- パスワードと TOTP 認証アプリケーションで認証した場合のサインインの成功
- 強制的な MFA の登録が必要な場合にパスワードと認証したサインインの成功
- パスワードのみを使用した認証で失敗したサインイン

パスワードのみを使用した認証での正常なサインイン

次の一連のイベントは、正常に完了したパスワードのみのサインインの例を示します。

CredentialChallenge（パスワード）


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-07T20:33:58Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
```

```
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "CredentialType":"PASSWORD"
   },
   "requestID":"5be44ffb-6946-4f47-acaf-1adebd4afead",
   "eventID":"27ea7725-c1fd-4355-bdba-d0e628e0e604",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```


成功 CredentialVerification（パスワード）


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-07T20:34:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
```

```
      "CredentialType":"PASSWORD"
   },
   "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
   "eventID":"c49640f6-0c8a-43d3-a6e0-900e3bb188d4",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```

成功 UserAuthentication（パスワードのみ）

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-07T20:34:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?
state=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
BshlIc5OBAA6ftz73M6LsfLWDlfOxviO2K3wet946lC30f_iWdilx-
zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7TqziOLiBLBUSx
east-1",
      "CredentialType":"PASSWORD"
```

```
   },
   "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
   "eventID":"e959a95a-2b33-478d-906c-4fe303e8a9f1",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```

外部の ID プロバイダーで認証した場合のサインインの成功

以下の一連のイベントは、外部の ID プロバイダを使用して SAML プロトコルで認証された場合のサインインの成功例を示しています。

成功 UserAuthentication（外部 ID プロバイダー）

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":""
   },
   "eventTime":"2020-12-07T20:34:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?
state=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
BshlIc5OBAA6ftz73M6LsfLWDlfOxviO2K3wet946lC30f_iWdilx-
```

```
zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7TqziOLiBLBUSx
east-1",
      "CredentialType":"EXTERNAL_IDP"
   },
   "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
   "eventID":"e959a95a-2b33-478d-906c-4fe303e8a9f1",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```


パスワードと TOTP 認証アプリケーションで認証した場合のサインインの成功

次の一連のイベントは、サインイン時に多要素認証が必要で、ユーザーがパスワードと TOTP 認証アプリケーションを使ってサインインに成功した例を示しています。

CredentialChallenge（パスワード）


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:13Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
```

```
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"PASSWORD"
   },
   "requestID":"e454ea66-1027-4d00-9912-09c0589649e1",
   "eventID":"d89cc0b5-a23a-4b88-843a-89329aeaef2e",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```

成功 CredentialVerification（パスワード）

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:20Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"PASSWORD"
   },
   "requestID":"92c4ac90-0d9b-452d-95d5-728487612f5e",
   "eventID":"4533fd49-6669-4d0b-b272-a0b2139309a8",
   "readOnly":false,
```

```
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```

CredentialChallenge (TOTP)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:20Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"TOTP"
   },
   "requestID":"92c4ac90-0d9b-452d-95d5-728487612f5e",
   "eventID":"29202f08-f240-40cc-b789-c0cea8a27847",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
```

```
   }
}
```

成功 CredentialVerification (TOTP)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:27Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"TOTP"
   },
   "requestID":"c40a691f-eeb1-4352-b286-5e909f96f318",
   "eventID":"e889ff1d-fcaf-454f-805d-7132cf2362a4",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```

成功 UserAuthentication（パスワード + TOTP)

```
{
```

```
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:27Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?state
\u003dQVlBQmVLeFhWeDRmZFJmMmxHcWYwdzhZck5RQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
\u0026auth_code
\u003d11Fir1mCVJ-4Y5UY6RI10UCXvRePCHd6195xvYg1rwo1Pj7B-7UGIGlYUUVe31Nkzd7ihxKn6DMdnFfO01O8qc3RF
Sx-pjBXKG_jUcvBk_UILdGytV4o1u97h42B-
TA_6uwdmJiw1dcCz_Rv44d_BS0PkulW-5LVJy1oeP1H0FPPMeheyuk5Uy48d5of9-c\u0026wdc_csrf_token
\u003dNMlui44guoVnxRd0qu2tYJIdyyFPX6SDRNTspIScfMM0AgFbho1nvvCaxPTghHbgHCRIXdffFtzH0sL1ow419Bobn
\u0026organization\u003dd-9067230c03\u0026region\u003dus-east-1",
      "CredentialType":"PASSWORD,TOTP"
   },
   "requestID":"c40a691f-eeb1-4352-b286-5e909f96f318",
   "eventID":"7a8c8725-db2f-488d-a43e-788dc6c73a4a",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```

強制的な MFA の登録が必要な場合にパスワードと認証したサインインの成功

次の一連のイベントは、パスワードによるサインインに成功した例ですが、ユーザーはサインインを完了する前に MFA デバイスの登録をリクエストされ、正常に完了しています。

CredentialChallenge（パスワード）


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-09T01:24:02Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "CredentialType":"PASSWORD"
   },
   "requestID":"321f4b13-42b5-4005-a0f7-826cad26d159",
   "eventID":"8c707b0f-e45a-4a9c-bee2-ff68638d2f1b",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```


成功 CredentialVerification（パスワード）

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-09T01:24:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "CredentialType":"PASSWORD"
   },
   "requestID":"12b57efa-0a92-4479-91a3-5b6641817c21",
   "eventID":"783b0c89-7142-4942-8b84-6ee0de1b992e",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```


成功 UserAuthentication（パスワード + MFA 登録が必要）


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
```

```
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-09T01:24:14Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?state
\u003dQVlBQmVGQ3VqdHF5aW9CUDdrNXRTVTJUaWNnQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
\u0026auth_code
\u003d11eZ80S_maUsZ7ABETjeQhyWfvIHYz52rgR28sYAKN1oEk2G07czrwzXvE9HLlN2K9De8LyBEV83SFeDQfrWpkwXf
FJyJqkoGrt_w6rm_MpAn0uyrVq8udY EgU3fhOL3QWvWiquYnDPMyPmmy_qkZgR9rz__BI
\u0026wdc_csrf_token
\u003dJih9U62o5LQDtYLNqCK8a6xj0gJg5BRWq2tbl75y8vAmwZhAqrgrgbxXat2M646UZGp93krw7WYQdHIgi5OYI9QSc
\u003dd-9067230c03\u0026region\u003dus-east-1",
      "CredentialType":"PASSWORD",
      "DeviceEnrollmentRequired":"true"
   },
   "requestID":"74d24604-a365-4237-8c4a-350795494b92",
   "eventID":"a15bf257-7f37-46c0-b67c-fea5fa6166be",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```


パスワードのみを使用した認証で失敗したサインイン

次の一連のイベントは、パスワードのみのサインインで失敗した例を示しています。

CredentialChallenge（パスワード）

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T18:56:15Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"adbf67c4-8188-4e2b-8527-fe539e328fa7",
      "CredentialType":"PASSWORD"
   },
   "requestID":"f54848ea-b1aa-402f-bf0d-a54561a2ffcc",
   "eventID":"d96f1d6c-dbd9-4a0b-9a45-6a2b66078c78",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```

失敗 CredentialVerification（パスワード）

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
```

```
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T18:56:21Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"adbf67c4-8188-4e2b-8527-fe539e328fa7",
      "CredentialType":"PASSWORD"
   },
   "requestID":"04528c82-a678-4a1f-a56d-ea2c6445a72a",
   "eventID":"9160fe06-fc2a-474f-9b78-000ee067a09d",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Failure"
   }
}
```


Amazon EventBridge

IAM Identity Center は Amazon と連携して EventBridge 、管理者が指定したアクションが組織内で発生したときにイベントを発生させることができます。例えば、アクションの重要性のため、ほとんどの管理者は、組織内に誰かが新しいアカウントを作成するたびに、またはメンバーアカウントの管理者が組織を離れようとするたびに警告を受けたいと考えています。これらのアクションを検索し、生成されたイベントを管理者定義のターゲットに送信する EventBridge ルールを設定できます。受信者に E メールまたはテキストメッセージを送信する Amazon SNS トピックをターゲットに指定できます。また、後で確認するためにアクションの詳細を口グに記録する AWS Lambda 関数を作成することもできます。

の設定と有効化の方法など EventBridge、 の詳細については、「Amazon EventBridge ユーザーガイド」を参照してください。

AD 同期エラーと設定可能な AD 同期エラーのログ記録

Active Directory (AD) 同期と設定可能な AD 同期設定のログ記録を有効にして、同期プロセス中に発生する可能性のあるエラーに関する情報を含むログを受信できます。これらのログを使用すると、AD 同期と設定可能な AD 同期に問題があるかどうかをモニタリングし、該当する場合はアクションを実行できます。ログは、Amazon CloudWatch Logs ロググループ、Amazon Simple Storage Service (Amazon S3) バケット、または Amazon S3 バケットと Firehose でサポートされているクロスアカウント配信を持つ Amazon Data Firehose に送信できます。

制限、アクセス許可、提供されるログの詳細については、「 からのログ記録の有効化 AWS のサービス」を参照してください。

> **Note**
>
> ログ記録には料金が発生します。詳細については、Amazon CloudWatch 料金ページの「販売済みログ」を参照してください。

AD 同期と設定可能な AD 同期エラーログを有効にするには

1. IAM Identity Center コンソール にサインインします。
2. [設定] を選択します。
3. 設定ページで、ID ソースタブを選択し、アクション を選択し、ログの管理 を選択します。
4. ログ配信の追加と、次のいずれかの送信先タイプを選択します。
   a. 「Amazon CloudWatch Logs へ」を選択します。次に、送信先ロググループを選択または入力します。
   b. Amazon S3へ」を選択します。次に、レプリケート先バケットを選択または入力します。
   c. Firehose を選択します。次に、送信先配信ストリームを選択または入力します。
5. [送信] を選択します。

AD 同期と設定可能な AD 同期エラーログを無効にするには

1. IAM Identity Center コンソール にサインインします。
2. [設定] を選択します。
3. 設定ページで、ID ソースタブを選択し、アクション を選択し、ログの管理 を選択します。

4. 削除する送信先の 削除 を選択します。
5. [送信] を選択します。

AD 同期と設定可能な AD 同期エラーログフィールド

考えられるエラーログフィールドについては、次のリストを参照してください。

`sync_profile_name`

同期プロファイルの名前。

`error_code`

発生したエラーのタイプを表すエラーコード。

`error_message`

発生したエラーに関する詳細情報を含むメッセージ。

`sync_source`

同期ソースは、エンティティが同期される場所です。IAM Identity Center の場合、これは によって管理される Active Directory (AD) です AWS Directory Service。同期ソースには、影響を受けるディレクトリのドメインと ARN が含まれます。

`sync_target`

同期ターゲットは、エンティティが保存される送信先です。IAM Identity Center の場合、これは Identity Store です。同期ターゲットには、影響を受ける Identity Store ARN が含まれています。

`source_entity_id`

エラーの原因となっているエンティティの一意の識別子。IAM Identity Center の場合、これはエンティティの SID です。

`source_entity_type`

エラーの原因となっているエンティティのタイプ。ここには、`USER` または `GROUP` が表示されます。

`eventTimestamp`

エラーが発生したときのタイムスタンプ。

AD 同期と設定可能な AD 同期エラーログの例

例 1: AD ディレクトリの期限切れパスワードのエラーログ

```
{
    "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"
}
```

例 2: 一意でないユーザー名を持つユーザーのエラーログ

```
{
    "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"
}
```

IAM Identity Center のコンプライアンス検証

サードパーティーの監査者は、複数の コンプライアンスプログラム AWS IAM Identity Center の一環として AWS のサービス などの のセキュリティと AWS コンプライアンスを評価します。

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、コンプライアンスプログラムAWS のサービス による対象範囲内のコンプライアンスプログラムを参照し、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、AWS 「コンプライアンスプログラム」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「 でのレポートのダウンロード AWS Artifact」の」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。 では、コンプライアンスに役立つ以下のリソース AWS を提供しています。

- セキュリティとコンプライアンスのクイックスタートガイド – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境 AWS を にデプロイする手順について説明します。
- アマゾン ウェブ サービスにおける HIPAA セキュリティとコンプライアンスのアーキテクチャ — このホワイトペーパーでは、企業が AWS を使用して HIPAA 対象アプリケーションを作成する方法について説明します。

  > **Note**
  >
  > すべて AWS のサービス HIPAA の対象となるわけではありません。詳細については、「HIPAA 対応サービスのリファレンス」を参照してください。

- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- AWS カスタマーコンプライアンスガイド — コンプライアンスの観点から責任共有モデルを理解します。このガイドでは、ガイダンスを保護し AWS のサービス 、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) を含む) のセキュリティコントロールにマッピングするためのベストプラクティスをまとめています。

- 「 デベロッパーガイド」の「 ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub – これにより AWS のサービス 、 内のセキュリティ状態を包括的に確認できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールのリストについては、「Security Hub のコントロールリファレンス」を参照してください。
- Amazon GuardDuty – これにより AWS アカウント、疑わしいアクティビティや悪意のあるアクティビティがないか環境を監視することで、、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービス を検出します。 GuardDuty は、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件への対応に役立ちます。
- AWS Audit Manager – これにより AWS のサービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

サポートされるコンプライアンス標準

IAM Identity Center は、以下の標準について監査済みであり、コンプライアンスの認定を取得する必要があるソリューションの一部として使用できます。

AWS は、医療保険の相互運用性と説明責任に関する法律 (HIPAA) コンプライアンスプログラムを拡張し、IAM Identity Center を HIPAA 対応サービス として含めました。

AWS は、 を使用して医療情報を処理および保存する方法の詳細について確認したいお客様向けに AWS のサービス 、HIPAA に重点を置いたホワイトペーパーを提供しています。詳細については、「HIPAA コンプライアンス」を参照してください。

オーストラリア政府の顧客は、情報セキュリティ登録評価プログラム (IRAP) を使用して、適切なコンプライアンス管理が行われていることを検証し、オーストラリアサイバーセキュリティセンター (ACSC) が作成したオーストラリア政府情報セキュリティマニュアル (ISM) の要件に対応する適切な責任モデルを決定することができます。詳細については、IRAP リソースを参照してください。

IAM Identity Center は、支払いカード業界 (PCI) のデータセキュリティ標準 (DSS) バージョン 3.2、サービスプロバイダーレベル 1 で準拠証明書を取得しています。

AWS 製品やサービスを使用してカード所有者データを保存、処理、または送信するお客様は、IAM Identity Center で次の ID ソースを使用して、独自の PCI DSS コンプライアンス証明書を管理できます。

- アクティブディレクトリ
- 外部 ID プロバイダー

IAM Identity Center の ID ソースは、現在 PCI DSS に準拠していません。

PCI コンプライアンスパッケージのコピーをリクエストする方法など、 AWS PCI DSS の詳細については、「PCI DSS レベル 1」を参照してください。

System and Organization Control (SOC) レポートとは、重要なコンプライアンスの統制および目標を IAM Identity Center がどのように達成したかを実証する、独立した第三者による審査報告書です。これらのレポートは、管理者と監査人が、運用とコンプライアンスの管理をどのようにサポートしているかを理解するのに役立ちます。SOC レポートには、次の 3 つのタイプがあります。

- AWS SOC 1 レポート - AWS Artifact でダウンロード
- AWS SOC 2: セキュリティ、可用性、機密性レポート - AWS Artifact でダウンロード
- AWS SOC 3: セキュリティ、可用性、機密性レポート

IAM Identity Center は、 AWS SOC 1、SOC 2、および SOC 3 レポートの対象です。詳細については、「SOC Compliance」(SOC コンプライアンス) を参照してください。

IAM Identity Center の障害への耐性

AWS グローバルインフラストラクチャは、 AWS リージョンとアベイラビリティーゾーンを中心に構築されています。 AWS リージョンは、低レイテンシー、高スループット、および冗長性の高いネットワークで接続された、物理的に分離された複数のアベイラビリティーゾーンを提供します。アベイラビリティーゾーンでは、アベイラビリティーゾーン間で中断せずに、自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、耐障害性、およびスケーラビリティが優れています。

AWS リージョンとアベイラビリティーゾーンの詳細については、AWS 「 グローバルインフラストラクチャ」を参照してください。

AWS IAM Identity Center 障害耐性の詳細については、「」を参照してください復元力設計とリージョンごとの動作。

IAM Identity Center でのインフラストラクチャのセキュリティ

マネージドサービスである AWS IAM Identity Center は、 AWS グローバルネットワークセキュリティで保護されています。 AWS セキュリティサービスと がインフラストラクチャ AWS を保護する方法については、AWS 「 クラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して AWS 環境を設計するには、「 Security Pillar AWS Well-Architected Framework」の「Infrastructure Protection」を参照してください。

が AWS 公開した API コールを使用して、ネットワーク経由で IAM Identity Center にアクセスします。クライアントは以下をサポートする必要があります:

- Transport Layer Security (TLS)。TLS 1.2 は必須で TLS 1.3 がお勧めです。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードは、Java 7 以降など、ほとんどの最新システムでサポートされています。

また、リクエストには、アクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、AWS Security Token ServiceAWS STS を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

AWS IAM Identity Center リソースのタグ付け

タグは、AWS リソースに追加して、リソースの識別、整理、検索を容易にできるカスタム属性ラベルです。各タグは 2 つの部分で構成されます。

- タグキー (例： `CostCenter`、`Environment`、または `Project`)。タグキーの長さは最大 128 文字で、大文字と小文字は区別されます。
- タグ値 (例: `111122223333` または `Production`)。タグ値の長さは最大 256 文字で、タグキーと同様に大文字と小文字は区別されます。タグの値を空の文字列に設定することはできますが、タグの値を null に設定することはできません。タグ値を省略すると、空の文字列を使用した場合と同じになります。

タグは、AWS リソースの識別や整理に役立ちます。多くの AWS のサービスではタグ付けがサポートされるため、さまざまなサービスからリソースに同じタグを割り当てて、リソースの関連を示すことができます。例えば、IAM アイデンティティセンターのインスタンスの特定のアクセス許可セットに同じタグを割り当てることができます。タグ付け方法の詳細については、「AWS 全般のリファレンスガイド」の「AWSリソースのタグ付け」と「タグ付けのベストプラクティス」を参照してください。

IAM Identity Center リソースの特定、整理、追跡に加え、IAM ポリシーのタグを使って、AWS リソースを表示および操作できるユーザーを制御することもできます。アクセスをコントロールするためのタグの使用については、「IAM ユーザーガイド」の「タグを使用した AWS リソースへのアクセスのコントロール」を参照してください。たとえば、ユーザが IAM Identity Center 権限セットを更新することを許可できるが、それは、IAM Identity Center 権限セットにそのユーザ名の値を持つ `owner` タグがある場合に限られます。

現在、タグは権限セットにのみ適用できます。IAM Identity Center が AWS アカウント で作成した対応するロールにはタグを適用できません。IAM Identity Center コンソール、AWS CLI、または IAM Identity Center API を使用して、権限セットのタ グを追加、編集、または削除できます。

以下のセクションでは、IAM Identity Center のタグに関する詳細を示します。

タグの制限

IAM Identity Center リソースのタグには、以下のような基本制限があります。

- リソースに割り当てることができるタグの最大数は 50 個です。

- キーの最大長は Unicode 文字で 128 文字です。
- 値の最大長は Unicode 文字で 256 文字です。
- タグのキーと値の有効な文字は次のとおりです。

  a-z、A-Z、0-9、スペース、および以下の文字： _ . : / = + -と@
- キーと値は大文字と小文字が区別されます。
- `aws:` をキーのプレフィックスとして使用しないでください。AWS 用に予約済みです。

IAM Identity Center コンソールを使用してタグを管理する

IAM アイデンティティセンターコンソールを使用して、インスタントまたはアクセス許可セットに関連付けられたタグを追加、編集、削除することができます。

IAM アイデンティティセンターコンソールの許可セットタグを管理するには

1. IAM Identity Center コンソールを開きます。
2. [アクセス許可セット] を選択します。
3. 管理するタグを含むアクセス権限セットの名前を選択します。
4. [権限] タブの [タグ] で以下のいずれかを行い、次のステップに進みます。
   a. このアクセス権限セットに既にタグが割り当てられている場合は、[タグの編集] を選択します。
   b. このアクセス権限セットにタグが割り当てられていない場合は、[タグの追加] を選択します。
5. それぞれの新しいタグについて、[Key] (キー) と [Value (optional)] (値 (オプション)) の列に値を入力します。完了したら、[Save changes] (変更の保存) を選択します。

タグを削除するには、削除したいタグの横にある [削除] 列の [X] をクリックします。

IAM アイデンティティセンターのインスタンスのタグを管理するには

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. [タグ] タブを選択します。

4. それぞれのタグについて、[Key] (キー) と [Value (optional)] (値 (オプション)) のフィールドに値を入力します。完了したら、[新しいタグを追加] ボタンを選択します。

タグを削除するには、削除したいタグの横にある [削除] ボタンを選択します。

AWS CLI の例

AWS CLI には、アクセス権限セットに割り当てたタグを管理するためのコマンドが用意されています。

タグの割り当て

アクセス権限セットにタグを割り当てるには、以下のコマンドを使用します。

Example **`tag-resource`** アクセス権限セットのコマンド

sso セットのコマンドの中で `tag-resource` を使って、アクセス権限セットにタグを割り当てます。

```
$ aws sso-admin tag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tags Stage=Test
```

このコマンドには次のパラメータが含まれます。

- `instance-arn` - オペレーションが実行される IAM アイデンティティセンター インスタンスの Amazon リソースネーム (ARN)。
- `resource-arn` — リストアップされるタグを含むリソースの ARN。
- `tags` – タグのキー/値ペア。

一度に複数のタグを割り当てるには、カンマ区切りリストで指定します。

```
$ aws sso-admin tag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tags Stage=Test,CostCenter=80432,Owner=SysEng
```

タグの表示

アクセス権限セットに割り当てたタグを表示するには、以下のコマンドを使用します。

Example **list-tags-for-resource** アクセス権限セットのコマンド

コマンドの sso セット内の list-tags-for-resource 使用して、アクセス権限セットにタグを割り当てます。

```
$ aws sso-admin list-tags-for-resource --resource-arn sso-resource-arn
```

タグの削除

アクセス権限セットからタグを削除するには、以下のコマンドを使用します。

Example **untag-resource** アクセス権限セットのコマンド

sso セットのコマンドの中で untag-resource を使って、アクセス権限セットからタグを削除します。

```
$ aws sso-admin untag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tag-keys Stage CostCenter Owner
```

--tag-keys パラメータには、1 つ以上のタグキーを指定します。タグ値は含めないでください。

権限セット作成時のタグの適用

アクセス権限セットにタグを作成するには、以下のコマンドを使用します。

Example **create-permission-set** コマンドとタグ

create-permission-set コマンドを使用してアクセス権限セットを作成するときは、--tags パラメータと共にタグを指定できます。

```
$ aws sso-admin create-permission-set \
> --instance-arn sso-instance-arn \
> --name permission=set-name \
> --tags Stage=Test,CostCenter=80432,Owner=SysEng
```

IAM Identity Center API を使用してタグを管理する

IAM Identity Center API の以下のアクションを使用して、アクセス権限セットのタグを管理することができます。

IAM Identity Center インスタンスタグの API アクション

次の API アクションを使用して、IAM アイデンティティセンターの許可セットまたはインスタンスのタグを割り当て、表示、削除します。

- TagResource
- ListTagsForResource
- UntagResource
- CreatePermissionSet
- CreateInstance

AWS CLI と IAM Identity Center の統合

AWS コマンドラインインターフェイス (CLI) バージョン 2 と IAM Identity Center の統合により、サインインプロセスが簡略化します。デベロッパーは、IAM Identity Center へのサインインに通常使用している Active Directory や IAM Identity Center の認証情報を用いて AWS CLI に直接サインインし、割り当てられたアカウントやロールにアクセスすることができます。例えば、管理者が IAM Identity Center を設定して認証に Active Directory を使用すると、デベロッパーは Active Directory の認証情報を使って AWS CLI に直接サインインすることができます。

AWS CLI と IAM Identity Center の統合により、以下のようなメリットがあります。

- 企業は、AWS Directory Service を使って IAM Identity Center を Active Directory に接続することで、IAM Identity Center や Active Directory からの認証情報を使ってデベロッパーがサインインできるようになります。
- デベロッパーは CLI からサインインすることで、より迅速なアクセスが可能になります。
- デベロッパーは、自分がアクセス権を割り当てたアカウントやロールを一覧表示して切り替えることができます。
- デベロッパーは、CLI 構成で名前付きロールプロファイルを自動的に生成し、保存し、CLI で参照することで、目的のアカウントやロールでコマンドを実行することができます。
- CLI は短期間の認証情報を自動的に管理するため、開発者は中断することなく安全に CLI を開始して使用し、長時間実行するスクリプトを実行することができます。

AWS CLI と IAM Identity Center の統合方法

AWS CLI と IAM Identity Center の統合を使用するためには、AWS Command Line Interface バージョン 2 をダウンロードし、インストールし、設定する必要があります。AWS CLI をダウンロードして IAM Identity Center と統合する方法の詳細な手順については、「AWS Command Line Interface ユーザーガイドの「IAM Identity Center を使用するためのAWS CLI の設定」を参照してください。

AWS IAM Identity Center リージョンの可用性

IAM ID センターには、 AWS リージョン一般的に使用されているものがいくつかあります。この可用性により、 AWS アカウント 複数のアプリケーションやビジネスアプリケーションへのユーザーアクセスを簡単に設定できます。 AWS ユーザがアクセスポータルにサインインすると、権限のあるアプリケーションを選択して、にアクセスできます AWS Management Console。 AWS アカウント IAM ID AWS リージョン センターがサポートしているすべてのリストについては、「IAM ID センターのエンドポイントとクォータ」を参照してください。

IAM Identity Center リージョン

最初に IAM Identity Center を有効にすると、IAM Identity Center で設定したすべてのデータが、設定したリージョンに保存されます。このデータには、ディレクトリ設定、権限セット、アプリケーションインスタンス、アプリケーションへのユーザー割り当てが含まれます。 AWS アカウント IAM Identity Center の ID ストアを使用している場合、IAM Identity Center で作成したすべてのユーザーとグループも同じリージョンに保存されます。IAM Identity Center は、無効にする必要のあるリージョンではなく、ユーザーが利用できるようにしておきたいリージョンにインストールすることをお勧めします。

AWS Organizations AWS リージョン 一度に 1 つしかサポートされません。IAM Identity Center を別のリージョンで有効にするには、まず現在の IAM Identity Center 設定を削除する必要があります。AWS 別のリージョンに切り替えるとアクセスポータルの URL も変わるため、すべての権限セットと割り当てを再設定する必要があります。

リージョン間の呼び出し

IAM Identity Center では、エンドユーザーがワンタイムパスワード (OTP) を第 2 認証要素として使用してサインインしようとした場合、Amazon Simple Email Service (Amazon SES) を使用して E メールを送信します。これらの E メールは、ユーザーが初期パスワードの設定、E メールアドレスの検証、パスワードのリセットを依頼されたときなど、特定の ID および認証情報の管理イベントでも送信されます。Amazon SES は IAM AWS リージョン アイデンティティセンターがサポートするサブセットで利用可能です。

IAM Identity Center は、Amazon SES が AWS リージョンでローカルで利用可能な場合に Amazon SES ローカルエンドポイントを呼び出します。Amazon SES がローカルで利用できない場合、IAM Identity Center は次の表に示すように、別の AWS リージョンで Amazon SES エンドポイントを呼び出します。

Amazon SES のリージョンコードは次の表のとおりです。

IAM Identity Center リージョンコード	IAM Identity Center リージョン名	Amazon SES リージョンコード	Amazon SES リージョン名
us-gov-east-1	AWS GovCloud (米国東部)	us-gov-west-1	AWS GovCloud (米国西部)
ap-east-1	アジアパシフィック (香港)	ap-northeast-2	アジアパシフィック (ソウル)
ap-southeast-4	アジアパシフィック (メルボルン)	ap-southeast-2	アジアパシフィック (シドニー)
ap-south-2	アジアパシフィック (ハイデラバード)	ap-south-1	アジアパシフィック (ムンバイ)
eu-central-2	欧州 (チューリッヒ)	eu-central-1	欧州 (フランクフルト)
eu-south-2	欧州 (スペイン)	eu-west-3	欧州 (パリ)
me-central-1	中東 (アラブ首長国連邦)	eu-central-1	欧州 (フランクフルト)

これらのクロスリージョン呼び出しでは、IAM Identity Center は次のユーザー属性を送信する場合があります。

- E メールアドレス
- [First name] (名)
- [Last name] (姓)
- アカウントイン AWS Organizations
- AWS アクセスポータル URL
- ユーザーネーム
- [ディレクトリ ID]
- ユーザー ID

オプトインリージョン (デフォルトでは無効になっているリージョン) での IAM ID センターの管理

ほとんどの場合 AWS リージョン 、 AWS すべてのサービスの操作がデフォルトで有効になっています。これらのリージョンは、IAM Identity Center で使用できるように自動的にアクティブ化されます。 AWS リージョン 以下はオプトインリージョンで、有効にする必要があります。

- アフリカ (ケープタウン)
- アジアパシフィック (香港)
- アジアパシフィック (ジャカルタ)
- アジアパシフィック (メルボルン)
- アジアパシフィック (ハイデラバード)
- 欧州 (ミラノ)
- 欧州 (チューリッヒ)
- 欧州 (スペイン)
- イスラエル (テルアビブ)
- 中東 (バーレーン)
- 中東 (アラブ首長国連邦)

オプトインで管理アカウントの IAM Identity Center を有効にすると AWS リージョン、すべてのメンバーアカウントの次の IAM Identity Center メタデータがリージョンに保存されます。

- アカウント ID
- アカウント名
- 連絡先 E メール
- IAM Identity Center がメンバーアカウントに作成する IAM ロールの Amazon リソースネーム (ARN)

IAM Identity Center がインストールされているリージョンを無効にすると、IAM Identity Center も無効になります。IAM Identity Center をリージョンで無効にすると、そのリージョンのユーザーはアプリケーションにシングルサインオンでアクセスできなくなります。 AWS アカウント AWS IAM ID センター設定内のデータは少なくとも 10 日間保持されます。この期間内に IAM Identity Center を再度有効にしても、IAM Identity Center の設定データはそのリージョンで引き続き利用できます。

オプトインで IAM Identity Center を再度有効にするには AWS リージョン、リージョンを再度有効にする必要があります。IAM Identity Center では一時停止中のイベントをすべて再処理する必要があるため、IAM Identity Center を再度有効にするとしばらく時間がかかる場合があります。

> **Note**
>
> IAM Identity Center で管理できるのは、 AWS アカウント での使用が有効になっているへのアクセスのみです。 AWS リージョン組織内のすべてのアカウントへのアクセスを管理するには、IAM Identity Center AWS リージョン で使用できるよう自動的にアクティベーションされる管理アカウントで IAM Identity Center を有効にします。

有効化と無効化の詳細については AWS リージョン、『ジェネラルリファレンス』の「管理 AWS リージョン」を参照してください。AWS

IAM Identity Center 設定を削除する

IAM Identity Center 構成を削除すると、その構成内のすべてのデータが削除され、復元することはできません。以下の表は、IAM Identity Center で設定されているディレクトリタイプに基づいて、どのようなデータが削除されるかを説明したものです。

削除されるデータについて	接続されているディレクトリ (AWS Managed Microsoft AD または AD Connector)	IAM Identity Center Identity Store
設定したすべての権限セット AWS アカウント	✓	✓
IAM Identity Center で設定したすべてのアプリケーション	✓	✓
AWS アカウント 設定したすべてのユーザ割り当てとアプリケーション	✓	✓

削除されるデータについて	接続されているディレクトリ (AWS Managed Microsoft AD または AD Connector)	IAM Identity Center Identity Store
ディレクトリまたはストア内のすべてのユーザーとグループ	該当なし	✓

現在の IAM Identity Center の設定を削除する必要がある場合は、以下の手順で行います。

IAM Identity Center 設定を削除するには

1. IAM Identity Center コンソールを開きます。
2. 左のナビゲーションペインの [設定] を選択します。
3. [設定] ページで、[管理] タブをクリックします。
4. [IAM Identity Center 設定の削除] セクションで、[削除] を選択します。
5. [IAM Identity Center 設定の削除] ダイアログで、データが削除されることを理解したことを示す各チェックボックスを選択します。テキストボックスに IAM Identity Center インスタンスを入力し、[確認] を選択します。

AWS IAM Identity Center クォータ

次の表では、IAM Identity Center 内のクォータについて説明します。クォータの増額リクエストは、管理者アカウントまたは委任管理者アカウントから行う必要があります。クォータの増加をリクエストするには、「クォータ増加のリクエスト」を参照してください。

> **Note**
>
> 50,000 人以上のユーザー、10,000 グループ、または 500 を超えるアクセス許可セットがある場合は、 AWS CLI と APIs を使用することをお勧めします。CLI の詳細については、AWS CLI と IAM Identity Center の統合 を参照してください。API の詳細については、「Welcome to the IAM Identity Center API Reference」参照してください。

アプリケーションクォータ

リソース	デフォルトのクォータ	引き上げ可能
サービスプロバイダーの SAML 証明書のファイルサイズ (PEM 形式)	2 KB	いいえ
SAML アサーションの制限	50,000 文字	いいえ
IAM Identity Center にアップロードされる IdP 証明書のファイルサイズの制限	UTF-8で 2500 文字	いいえ
アプリケーションごとのアクセススコープ	25	いいえ

AWS アカウント クォータ

リソース	デフォルトのクォータ	引き上げ可能
IAM Identity Center で許可される許可セット数	2000	はい
ごとに許可されるプロビジョニングされたアクセス許可セットの数 AWS アカウント	250	はい
アクセス権限セットあたりのインラインポリシーの数	1	いいえ
アクセス許可セットあたりの AWS マネージドポリシーとカスタマーマネージドポリシーの数	20[1]	いいえ
アクセス権限セットあたりのインラインポリシーの最大サイズ	32,768 バイト 権限セットごとのインラインポリシー内の空白以外の文字の最大サイズは 10,240 バイトです。	いいえ
で一度に更新できる IAM AWS アカウント ロール (アクセス許可セット) の数	1	いいえ

[1]AWS Identity and Access Management (IAM) は、ロールごとに 10 個の管理ポリシーのクォータを設定します。このクォータを活用するには、アクセス許可セットをデプロイ AWS アカウント する各 の Service Quotas コンソールで、IAM ロールにアタッチされた IAM クォータ管理ポリシーの引き上げをリクエストします。

> **Note**
>
> アクセス権限セット は、 で IAM ロール AWS アカウント としてプロビジョニングされるか、 で既存の IAM ロールを使用するため AWS アカウント、IAM クォータに従います。IAM ロールに関する IAM クォータの詳細については、「IAM と STS クォータ」 を参照してください。

Active Directory のクォータ

リソース	デフォルトのクォータ	引き上げ可能
一度に実現できる接続ディレクトリの数	1	いいえ

IAM Identity Center Identity Store クォータ

リソース	デフォルトのクォータ	引き上げ可能
IAM Identity Center でサポートされるユーザーの数	100000	はい
IAM Identity Center でサポートされるグループの数	100000	いいえ
ユーザーの許可を評価するために使用できる一意のグループの数	1,000	いいえ

IAM Identity Center のスロットル制限

リソース	デフォルトのクォータ
IAM Identity Center API	「IAM Identity Center API」のコレクティブスロットルは、最大毎秒 20 トランザクション

リソース	デフォルトのクォータ
	(TPS) です。の未処理の非同期呼び出しの最大レートCreateAccountAssignmentは 10 です。これらのクォータは変更できません。

追加のクォータ

リソース	デフォルトのクォータ	引き上げ可能
設定できる AWS アカウントまたはアプリケーションの合計数 *	3000	はい
IAM アイデンティティセンターのアカウントごとの合計インスタンス数	1	いいえ
信頼できるトークン発行者の総数	10	いいえ

* 最大 3000 AWS アカウント のアプリケーション (合計) がサポートされています。例えば、2,750 個のアカウントと 250 個のアプリケーションを設定し、合計 3,000 個のアカウントとアプリケーションを設定することができます。

IAM Identity Center の問題のトラブルシューティング

以下は、IAM Identity Center コンソールを設定または使用するときに発生する可能性のある問題のトラブルシューティングに役立ちます。

IAM アイデンティティセンターのアカウントインスタンスの作成に関する問題

IAM アイデンティティセンターのアカウントインスタンスを作成する場合、いくつかの制限が適用される場合があります。IAM Identity Center コンソールからアカウントインスタンスを作成できない場合、またはサポートされている AWS マネージドアプリケーションのセットアップエクスペリエンスで、次のユースケースを確認します。

- アカウントインスタンスを作成しようとしている AWS リージョン AWS アカウント の他の を確認します。IAM アイデンティティセンターのインスタンスは AWS アカウントにつき 1 つに制限されています。アプリケーションを有効にするには、IAM Identity Center のインスタンス AWS リージョン を使用して に切り替えるか、IAM Identity Center のインスタンスなしで アカウントに切り替えます。
- 組織が 2023 年 9 月 14 日より前に IAM Identity Center を有効にしている場合、管理者はアカウントインスタンスの作成をオプトインする必要がある場合があります。管理者と協力して、管理アカウントの IAM アイデンティティセンターコンソールからアカウントインスタンスを作成できるようにします。
- 管理者が IAM アイデンティティセンターのアカウントインスタンスの作成を制限するサービスコントロールポリシーを作成した可能性があります。管理者と協力してアカウントを許可リストに追加します。

IAM アイデンティティセンターと連携するように事前設定されているクラウドアプリケーションのリストを表示しようとすると、エラーが表示されます。

以下のエラーは、`sso:ListApplications` は許可するが、他の IAM アイデンティティセンター API は許可しないポリシーがある場合に発生します。ポリシーを更新してこのエラーを解決します。

`ListApplications` アクセス許可は複数の API を承認します。

- ListApplications API。
- IAM アイデンティティセンターコンソールで使用される ListApplicationProviders API に似た内部 API。

重複を解決するために、内部 API も ListApplicationProviders アクションの使用を許可するようになりました。パブリック ListApplications API を許可し、内部 API を拒否するには、ポリシーに ListApplicationProviders アクションを拒否するステートメントを含める必要があります。

```
      "Statement": [
    {
         "Effect": "Deny",
         "Action": "ListApplicationProviders",
         "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": "ListApplications",
        "Resource": "<instanceArn>" // (or "*" for all instances)
    }
]
```

内部 API を許可して ListApplications を拒否するには、ポリシーで ListApplicationProviders のみ許可する必要があります。ListApplications API は明示的に許可されない場合は拒否されます。

```
      "Statement": [
    {
         "Effect": "Allow",
         "Action": "ListApplicationProviders",
         "Resource": "*"
    }
]
```

ポリシーが更新されたら、 AWS Support に連絡して、このプロアクティブメジャーを削除します。

IAM Identity Center によって作成された SAML アサーションの内容に関する問題

IAM Identity Center は、 AWS アクセスポータルから AWS アカウント および SAML アプリケーションにアクセスするときに、IAM Identity Center によって作成および送信される SAML アサーションのウェブベースのデバッグエクスペリエンスを提供します。これには、これらのアサーション内の属性が含まれます。IAM Identity Center が生成する SAML アサーションの詳細を確認するには、以下の手順を行います。

1. AWS アクセスポータルにサインインします。
2. ポータルにサインインしている状態で、Shift キーを押しながらアプリケーションタイルを選択し、Shift キーを離します。
3. [You are now in administrator mode] (現在、管理者モードです) ページの情報を調べます。この情報を保存しておきたい場合は、[Copy XML] をクリックして、その内容を別の場所に貼り付けます。
4. [Send to <application>] (<アプリケーション>に送信する) をクリックして続けます。このオプションは、アサーションをサービスプロバイダに送信します。

> **Note**
>
> ブラウザの設定やオペレーティングシステムによっては、この手順をサポートしていない場合があります。この手順は、Firefox、Chrome、Edge ブラウザを使用して Windows 10 で評価されています。

特定のユーザーが、外部の SCIM プロバイダーからの IAM Identity Center に同期できません

IAM Identity Center へのプロビジョニングのために IdP で構成されたユーザーのサブセットに対して SCIM 同期が成功し、他のユーザーに対して失敗する場合、ID プロバイダーから `'Request is unparsable, syntactically incorrect, or violates schema'` と同じようなエラーが表示されることがあります。また、 に詳細なプロビジョニング失敗メッセージが表示される場合があります AWS CloudTrail。

この問題は、IAM Identity Center がサポートしていない方法で IdP のユーザーが設定されているためです。IAM Identity Center SCIM 実装の詳細 (ユーザーオブジェクトに必要なパラメータ、オプションのパラメータ、禁止されたパラメータ、操作の仕様など) は、「IAM Identity Center SCIM 実装デベロッパーガイド」に記載されています。「SCIM デベロッパーガイド」の SCIM 要件に関する情報は信頼できると考えなければなりません。しかし、このエラーが発生する一般的な理由は以下の通りです。

1. IdP のユーザーオブジェクトには、名 (given)、姓 (family)、表示名がありません。

   - 解決策: ユーザーオブジェクトのための、名 (given)、姓 (family)、表示名を追加します。さらに、IdP のユーザーオブジェクトに対する SCIM プロビジョニングマッピングが、これらの属性すべてに対して空ではない値を送信するように構成されていることを確認してください。

2. 1 つの属性に対して複数の値がユーザーに送信されています (「マルチバリュー属性」とも知られています)。例えば、ユーザーが IdP で職場と自宅の両方の電話番号を指定していたり、複数の E メールや実際の住所を指定していたりする場合、IdP はその属性の複数またはすべての値を同期するように設定されています。

   - ソリューションオプション:

     i. IdP のユーザーオブジェクトに対する SCIM プロビジョニングマッピングを更新して、特定の属性に対して単一の値のみを送信するようにします。例えば、各ユーザーの職場の電話番号のみを送信するマッピングを設定します。

     ii. IdP でユーザーオブジェクトから追加属性を安全に削除できる場合は、追加値を削除して、ユーザーのその属性に設定された値を 1 つまたは完全に無くすことができます。

     iii. 属性が のアクションに必要ない場合は AWS、IdP のユーザーオブジェクトの SCIM プロビジョニングマッピングからその属性のマッピングを削除します。

3. お客様の IdP は、複数の属性に基づいてターゲット (ここでは IAM Identity Center) のユーザーをマッチさせようとします。ユーザー名は、特定の IAM Identity Center インスタンス内で一意であることが保証されているため、マッチングに使用する属性として `username` 指定するだけです。

   - 解決策: IdP の SCIM 構成が、IAM Identity Center でのユーザーとのマッチングに単一の属性のみを使用していることを確認します。例えば、IAM Identity Center へのプロビジョニングのために、IdP の `username` または `userPrincipalName` を SCIM の `userName` 属性にマッピングすることは、ほとんどの実装で十分に要件を満たします。

ユーザー名が UPN 形式の場合、ユーザーはサインインできません

ユーザーは、サインインページでユーザー名を入力するために使用する形式に基づいて、 AWS アクセスポータルにサインインできない場合があります。ほとんどの場合、ユーザーはプレーンユーザー名、ダウンレベルログオン名 (DOMAIN\UserName) 、または UPN ログオン名 () を使用してユーザーポータルにサインインできますUserName@Corp.Example.com。ただし、IAM Identity Center が MFA を有効にした接続ディレクトリを使用しており、検証モードが Context-aware または Always-on のいずれかに設定されている場合は例外です。このシナリオでは、ユーザーはダウンレベルログオン名 (DOMAIN\) でサインインする必要がありますUserName。詳細については、「Identity Center ユーザー用の多要素認証」を参照してください。アクティブディレクトリへのサインインに使用されるユーザー名の形式についての一般的な情報は、Microsoft のドキュメントサイトの「User Name Formats」(ユーザー名形式) を参照してください。

IAM ロールを変更すると、「Cannot perform the operation on the protected role」(保護されたロールでオペレーションを実行できません) というエラーが発生する

アカウントで IAM ロールを確認すると、ロール名がAWSReservedSSO「_」で始まることがあります。これらは、IAM Identity Center サービスがアカウントに作成したロールであり、アカウントにアクセス権限セットを割り当てたものです。IAM コンソール内からこれらのロールを変更しようとすると、次のエラーが発生します。

```
'Cannot perform the operation on the protected role 'AWSReservedSSO_RoleName_Here' -
 this role is only modifiable by AWS'
```

これらのロールは、 の管理アカウントにある IAM Identity Center 管理者コンソールからのみ変更できます AWS Organizations。変更後は、割り当てられている AWS アカウントに変更を反映させることができます。

ディレクトリユーザーが、パスワードをリセットできません

アクセス AWS ポータルのサインイン時に、ディレクトリユーザーがパスワードを忘れた場合? オプションを使用してパスワードをリセットする場合、新しいパスワードは、「」で説明されているデフォルトのパスワードポリシーに従う必要がありますIAM Identity Center で ID を管理する際のパスワード要件。

ユーザーがポリシーに準拠するパスワードを入力し、エラー を受け取った場合は`We couldn't update your password`、失敗 AWS CloudTrail が記録されているかどうかを確認します。これは、次のフィルター CloudTrail を使用して のイベント履歴コンソールで検索することで実行できます。

```
"UpdatePassword"
```

メッセージに次のように記載されている場合は、サポートに連絡する必要があります。

```
"errorCode": "InternalFailure",
      "errorMessage": "An unknown error occurred“
```

この問題の別の原因として、ユーザー名の値が命名規則に反していることが考えられます。命名規則は、「surname.givenName」などの特定のパターンに従う必要があります。しかし、ユーザー名の中には非常に長いものや特殊な文字を含むものがあり、API コールの中で文字が抜けてしまい、エラーになってしまうことがあります。同じ方法でテストユーザーとパスワードのリセットを試みて、これが当てはまるかどうかを確認することもできます。

問題が解決しない場合は、AWS サポートセンターまでお問い合わせください。

ユーザーはアクセス権限セットを参照しているが、割り当てられたアカウントやアプリケーションにアクセスできません

この問題は、クロスドメイン ID 管理 (SCIM) システムを外部の ID プロバイダーで使用している場合に発生します。具体的には、ユーザーまたはユーザーが所属していたグループが削除された後、ID プロバイダーで同じユーザー名 (ユーザーの場合) または名前 (グループの場合) を使用して再作成された場合、IAM Identity Center では新しいユーザーまたはグループに新しい一意の内部識別子が作成されます。しかし、IAM Identity Center は権限データベースに古い識別子への参照を保持しているため、ユーザーやグループの名前は UI に表示されますが、アクセスは失敗します。これは、UI が参照するときのベースとなるユーザーまたはグループ ID がもはや存在しないためです。

この場合の AWS アカウント アクセスを復元するには、最初に割り当てられた AWS アカウント(s) から古いユーザーまたはグループのアクセスを削除し、そのユーザーまたはグループにアクセスを再割り当てします。これにより、新しいユーザーまたはグループの正しい識別子でアクセス権限セットが更新されます。同様に、アプリケーションのアクセス権を回復するには、そのアプリケーションの割り当てユーザーリストからそのユーザーまたはグループのアクセス権を削除し、その後、そのユーザーまたはグループを再び追加します。

また、問題のユーザーまたはグループの名前を参照する SCIM 同期イベントを CloudTrail ログで検索して、障害が AWS CloudTrail 記録されたかどうかを確認することもできます。

アプリケーションカタログからアプリケーションを正しく設定できない

IAM アイデンティティセンターのアプリケーションカタログからアプリケーションを追加した場合は、各サービスプロバイダーが独自の詳細なドキュメントを提供していることに注意してください。この情報は、IAM アイデンティティセンターコンソール上でアプリケーションの [設定] タブから確認できます。

問題が、サービスプロバイダーのアプリケーションと IAM Identity Center の間の信頼関係の設定に関係している場合は、必ず手順書でトラブルシューティングのステップを確認してください。

ユーザーが外部の ID プロバイダーを使用してサインインしようとすると、「予期しないエラーが発生しました」というエラーが発生します

このエラーは複数の理由で発生する可能性がありますが、よくあるのは、SAML リクエストで送信したユーザー情報と IAM Identity Center でのユーザー情報との間にミスマッチがあることが挙げられます。

IAM Identity Center のユーザーが、外部の IdP を ID ソースとして使用しているときに正常にサインインするためには、以下の条件を満たす必要があります。

- SAML nameID 形式 (アイデンティティプロバイダーで設定) は「E メール」でなければなりません。
- nameID の値は、適切に (RFC2822) でフォーマットされた文字列である必要があります (user@domain.com)
- nameID の値は、IAM Identity Center の既存ユーザーのユーザー名と完全に一致する必要があります (IAM Identity Center のメールアドレスが一致するかどうかは問題ではありません - インバウンドマッチはユーザー名に基づいて行われます)。
- SAML 2.0 フェデレーションの IAM Identity Center　実装では、ID プロバイダーと IAM Identity Center　間の SAML レスポンスで 1 つのアサーションのみがサポートされます。暗号化された SAML アサーションはサポートされていません。

- 以下の記述は、IAM Identity Center アカウントで アクセスコントロールの属性 が有効になっている場合に適用されます。
  - SAML リクエストでマッピングされる属性の数は、50 以下でなければなりません。
  - SAML リクエストに複数の値を持つ属性を含めることはできません。
  - SAML リクエストには、同じ名前の複数の属性を含めることはできません。
  - 属性の値として、構造化された XML を含んではいけません。
  - Name の形式は、汎用的な形式ではなく、SAML で指定された形式でなければなりません。

> **Note**
>
> IAM Identity Center は、SAML フェデレーションを介した新しいユーザーやグループの「ジャストインタイム」での作成はできません。つまり、IAM Identity Center にサインインするためには、手動または自動プロビジョニングによって、ユーザーが IAM Identity Center であらかじめ作成されている必要があります。

このエラーは、ID プロバイダーで構成されたアサーションコンシューマサービス (ACS) のエンドポイントが、IAM Identity Center インスタンスで提供された ACS の URL と一致しない場合にも発生します。この 2 つの値が正確に一致するようにしてください。

さらに、 にアクセスしてイベント名 ExternalIdPDirectoryLogin でフィルタリングすることで AWS CloudTrail 、外部 ID プロバイダーのサインインエラーをさらにトラブルシューティングできます。

エラー「アクセスコントロールのための属性の有効化に失敗しました」

このエラーは、ABAC を有効にしているユーザーが、アクセスコントロールの属性 を有効にするために必要な `iam:UpdateAssumeRolePolicy` 権限を持っていない場合に発生することがあります。

MFA にデバイスを登録しようとすると、「Browser not supported」(サポートされていないブラウザ) というメッセージが表示されます。

WebAuthn は現在、Google Chrome、Mozilla Firefox、Microsoft Edge、Apple Safari ウェブブラウザ、Windows 10 および Android プラットフォームでサポートされています。macOS および iOS ブラウザでのプラットフォーム認証サポートなど、サポートの一部のコンポーネント WebAuthn はさまざまです。ユーザーがサポートされていないブラウザまたはプラットフォームに WebAuthn デバイスを登録しようとすると、サポートされていない特定のオプションがグレー表示されます。または、サポートされているすべてのメソッドがサポートされていないというエラーが表示されます。このような場合、ブラウザ/プラットフォームのサポートの詳細については、FIDO2: ウェブ認証 (WebAuthn) 」を参照してください。IAM Identity Center WebAuthn の の詳細については、「」を参照してくださいFIDO2 認証機能。

アクティブディレクトリの「ドメインユーザー」グループが IAM Identity Center に正しく同期しない

アクティブディレクトリのドメインユーザーグループは、AD ユーザーオブジェクトのデフォルトの「プライマリグループ」です。アクティブディレクトリのプライマリグループとそのメンバシップは、IAM Identity Center では読み取れません。IAM Identity Center リソースまたはアプリケーションへのアクセスを割り当てる際には、グループメンバーシップが IAM Identity Center ID ストアに適切に反映されるように、ドメインユーザーグループ (またはプライマリグループとして割り当てられた他のグループ) 以外のグループを使用してください。

無効な MFA 認証情報エラー

このエラーは、SCIM プロトコルを使用してアカウントが IAM Identity Center に完全にプロビジョニングされる前に、ユーザーが外部 ID プロバイダー (Okta または Microsoft Entra ID など) のアカウントを使用して IAM Identity Center にサインインしようとすると発生する可能性があります。ユーザーアカウントが IAM Identity Center にプロビジョニングされると、この問題は解決します。アカウントが IAM Identity Center にプロビジョニングされていることを確認します。されていない場合は、外部 ID プロバイダーのプロビジョニングログを確認します。

認証アプリケーションを使って登録やサインインをしようとすると、「予期しないエラーが発生しました」というメッセージが表示されます

コードベースの認証アプリケーションと組み合わせて IAM Identity Center で使用されるような、タイムベースドワンタイムパスワード (TOTP) システムは、クライアントとサーバー間の時間の同期に依存しています。認証システムのアプリケーションをインストールしているデバイスが信頼できるタイムソースに正しく同期されていることを確認するか、またはデバイスの時間を、NIST (https://www.time.gov/) やその他のローカル/地域など、信頼できるソースと一致するように手動で設定してください。

IAM Identity Center にサインインしようとすると、「ユーザーではありません。エラーです」と表示されます。

このエラーは、IAM Identity Center のインスタンス、または IAM Identity Center が ID ソースとして使用している外部 ID プロバイダー (IdP) にセットアップの問題があることを示します。以下を確認することをお勧めします。

- サインインに使用しているデバイスの日付と時刻の設定を確認します。日付と時刻を自動的に設定することをお勧めします。これが利用できない場合は、日付と時刻を既知の Network Time Protocol (NTP) サーバーに同期することをお勧めします。
- IAM Identity Center にアップロードされた IdP 証明書が、IdP によって提供された証明書と同じであることを確認します。IAM Identity Center コンソールから証明書を確認するには、設定 に移動します。ID ソースタブでアクション を選択し、認証の管理 を選択します。IdP 証明書と IAM Identity Center 証明書が一致しない場合は、新しい証明書を IAM Identity Center にインポートします。
- ID プロバイダーのメタデータファイル内の NameID 形式が以下であることを確認します。
  - `urn:oasis:name:tc:SAML:1.1:nameid-format:emailAddress`
- から ID プロバイダー AWS Directory Service として AD Connector を使用している場合は、サービスアカウントの認証情報が正しく、有効期限が切れていないことを確認します。詳細については、「 で AD Connector サービスアカウントの認証情報 AWS Directory Serviceを更新する」を参照してください。

ユーザーが IAM Identity Center からのメールを受信できません

IAM Identity Center サービスで送信されるすべてのメールは、アドレス `no-reply@signin.aws` または `no-reply@login.awsapps.com` のいずれかから送信されます。メールシステムは、これらの送信者 E メールアドレスからの E メールを受け入れ、迷惑メールやスパムとして処理しないように設定する必要があります。

エラー: 管理アカウントにプロビジョニングされたアクセス権限セットを削除/変更/削除/割り当てることはできません

このメッセージは、委任された管理この機能が有効になっていること、および以前に試行したオペレーションは、 で管理アカウントのアクセス許可を持つユーザーのみが正常に実行できることを示します AWS Organizations。この問題を解決するには、これらのアクセス許可を持つユーザーとしてサインインし、タスクを再度実行するか、正しいアクセス許可を持つユーザーにこのタスクを割り当てます。詳細については、「メンバーアカウントを作成する」を参照してください。

エラー: セッショントークンが見つからないか無効です

このエラーは、ウェブブラウザ、 AWS Toolkit、 などのクライアントが AWS CLIサーバー側で取り消されたセッションを使用しようとしたときに発生する可能性があります。この問題を修正するには、クライアントアプリケーションまたはウェブサイトに戻り、プロンプトが表示されたら再度ログインするなど、もう一度試してください。これには、IDE AWS Toolkit 内の からの保留中の接続試行など、保留中のリクエストをキャンセルする必要が生じる場合があります。

ドキュメント履歴

次の表に、 AWS IAM Identity Center ドキュメントへの重要な追加点を示します。また、お客様からいただいたフィードバックに対応するために、ドキュメントを頻繁に更新しています。

- 主要なドキュメントの最終更新日: 2022 年 9 月 23 日

変更	説明	日付
AWS 管理ポリシーの更新	`AWSIAMIdentityCenterAllowListForIdentityContext` AWS 管理ポリシーのアクセス許可を更新しました。	2024 年 5 月 17 日
AWS 管理ポリシーの更新	`AWSIAMIdentityCenterAllowListForIdentityContext` AWS 管理ポリシーのアクセス許可を更新しました。	2024 年 4 月 30 日
AWS 管理ポリシーの更新	`AWSSSOMasterAccountAdministrator` AWS 管理ポリシーのアクセス許可を更新しました。	2024 年 4 月 26 日
AWS 管理ポリシーの更新	`AWSSSOMemberAccountAdministrator` AWS 管理ポリシーのアクセス許可を更新しました。	2024 年 4 月 26 日
AWS 管理ポリシーの更新	`AWSSSOReadOnly` AWS 管理ポリシーのアクセス許可を更新しました。	2024 年 4 月 26 日
AWS 管理ポリシーの更新	`AWSIAMIdentityCenterAllowListForIden`	2024 年 4 月 26 日

	tityContext AWS 管理ポリシーのアクセス許可を更新しました。	
AWS 管理ポリシーの更新	AWSIAMIdentityCenterAllowListForIdentityContext AWS 管理ポリシーのアクセス許可を更新しました。	2024 年 4 月 24 日
AWS 管理ポリシーの更新	AWSIAMIdentityCenterAllowListForIdentityContext AWS 管理ポリシーのアクセス許可を更新しました。	2024 年 4 月 19 日
AWS 管理ポリシーの更新	AWSIAMIdentityCenterAllowListForIdentityContext AWS 管理ポリシーのアクセス許可を更新しました。	2024 年 4 月 11 日
AWS 管理ポリシーの更新	AWSIAMIdentityCenterAllowListForIdentityContext AWS 管理ポリシーのアクセス許可を更新しました。	2023 年 11 月 26 日
新しい AWS マネージドポリシーのトピック	AWSIAMIdentityCenterAllowListForIdentityContext AWS 管理ポリシーの詳細を追加しました。	2023 年 11 月 15 日
IAM Identity Center の使用を開始するためのガイダンスの強化	IAM Identity Center の使用開始と管理ユーザーの作成に関する新しいコンテンツを追加しました。	2022 年 9 月 23 日

Identity Center API リファレンスのユーザーとグループが更新されました	この更新には、Identity Center API リファレンスガイドの新しい「API の作成、更新、削除」への参照が含まれます。	2022 年 8 月 31 日
AWS Single Sign-On (AWS SSO) の名前が AWS IAM Identity Center に変更されました	AWS に が導入されました AWS IAM Identity Center。IAM Identity Center は、AWS Identity and Access Management (IAM) の機能を拡張して、ワークフォースユーザーのアカウントとアプリケーションへのアクセスを一元管理できるようにします。IAM Identity Center の機能には、アプリケーション割り当て、マルチアカウント権限、 AWS アクセスポータルなどがあります。	2022 年 7 月 26 日
権限セットにおける権限境界と顧客管理ポリシーをサポート	アクセス許可セットで AWS マネージドポリシーとカスタマーマネージド AWS Identity and Access Management (IAM) ポリシーを使用するためのコンテンツを追加しました。	2022 年 7 月 14 日
手動で有効にした AWS リージョンのサポート	手動で有効化されたリージョンで IAM Identity Center を使用するコンテンツが追加されました。	2022 年 6 月 15 日
AWS 管理ポリシーの更新	`AWSSSOServiceRolePolicy` AWS 管理ポリシーのアクセス許可を更新しました。	2022 年 5 月 11 日

委任された管理者のサポートを追加	委任管理機能のコンテンツが追加されました。	2022 年 5 月 11 日
AWS 管理ポリシーの更新	`AWSSSOMasterAccountAdministrator` 、、 `AWSSSOMemberAccountAdministrator` `AWSSSOReadOnly` AWS マネージドポリシーのアクセス許可を更新しました。	2022 年 4 月 28 日
設定可能な AD 同期をサポート	設定可能な AD 同期機能のコンテンツが追加されました。	2022 年 4 月 14 日
新しい AWS マネージドポリシーのトピック	`AWSSSOMasterAccountAdministrator` AWS マネージドポリシーの詳細を追加しました。	2021 年 8 月 4 日
クォータの更新	クォータテーブルを調整しました。	2020 年 12 月 21 日
新しいポリシーの例	新しいカスタマーマネージドポリシーの例を追加し、必要な権限のセクションを更新しました。	2020 年 12 月 21 日
属性ベースのアクセス制御 (ABAC) のサポート	ABAC 機能のコンテンツを追加しました。	2020 年 11 月 24 日
MFA 強制登録のサポート	サインイン時に MFA デバイスの登録をリクエストするための更新です。	2020 年 11 月 23 日
のサポート WebAuthn	新しい WebAuthn 機能のコンテンツが追加されました。	2020 年 11 月 20 日

Ping ID のサポート	サポートされている外部 ID プロバイダーとして Ping Identity 製品と統合するためのコンテンツを追加しました。	2020 年 10 月 26 日
のサポート OneLogin	サポートされている外部 ID プロバイダーとして OneLogin と統合するためのコンテンツを追加しました。	2020 年 7 月 31 日
Okta のサポート	サポートされている外部 ID プロバイダーとして Okta と統合するためのコンテンツを追加しました。	2020 年 5 月 28 日
外部 ID プロバイダーのサポート	ディレクトリから ID ソースへの参照を変更し、外部の ID プロバイダーをサポートするコンテンツを追加しました。	2019 年 11 月 26 日
新しい MFA 設定	2 段階認証のトピックを削除し、代わりに新しい MFA のトピックを追加しました。	2019 年 10 月 24 日
2 段階認証を追加するための新しい設定	ユーザーの 2 段階認証を有効にする方法について、コンテンツを追加しました。	2019 年 1 月 16 日
AWS アカウントでのセッション期間のサポート	AWS アカウントのセッション期間を設定する方法に関するコンテンツを追加しました。	2018 年 10 月 30 日
Identity Center ディレクトリを使用する新しいオプション	Identity Center ディレクトリを選択するか、既存の AD ディレクトリに接続するためのコンテンツを追加しました。	2018 年 10 月 17 日

アプリケーションでのリレーステートとセッションの有効期間のサポート	アプリケーションのリレー状態とセッションの有効期間に関するコンテンツを追加しました。	2018 年 10 月 10 日
新しいアプリケーションの追加サポート	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, と UserEcho をアプリケーションカタログに追加しました。	2018 年 8 月 3 日
管理アカウントへのマルチアカウントアクセスのサポート	管理アカウントでユーザーにマルチアカウントアクセスを委任する方法に関するコンテンツを追加しました。	2018 年 7 月 9 日
新しいアプリケーションのサポート	DocuSign, Keeper Security, と SugarCRM をアプリケーションカタログに追加しました。	2018 年 3 月 16 日
CLI アクセスの一時認証情報の取得	AWS CLI コマンドを実行するための一時的な認証情報を取得する方法に関する情報を追加しました。	2018 年 2 月 22 日

新しいガイド	これは IAM Identity Center ユーザーガイドの最初のリリースです。	2017 年 12 月 7 日

AWS 用語集

AWS の最新の用語については、「AWS の用語集リファレンス」の「AWS 用語集」を参照してください。

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。