Guide de l’utilisateur

AWS IAM Identity Center

AWS IAM Identity Center: Guide de l’utilisateur

Table of Contents

Qu'est-ce que IAM Identity Center ?

AWS IAM Identity Center est recommandé Service AWS pour gérer l'accès des utilisateurs humains aux AWS ressources. Il s'agit d'un endroit unique où vous pouvez attribuer aux utilisateurs de votre personnel un accès cohérent à plusieurs applications Comptes AWS et applications. workforce identities L'IAM Identity Center est proposé sans frais supplémentaires.

Avec IAM Identity Center, vous pouvez créer ou connecter des utilisateurs du personnel et gérer de manière centralisée leur accès à toutes leurs Comptes AWS applications. Vous pouvez utiliser des autorisations multi-comptes pour attribuer aux utilisateurs de votre personnel l'accès à Comptes AWS. Vous pouvez utiliser les attributions d'applications pour attribuer à vos utilisateurs l'accès aux applications AWS gérées et aux applications gérées par le client.

> **Note**
>
> Bien que le nom AWS de service Single Sign-On ait été retiré, le terme « authentification unique » est toujours utilisé dans ce guide pour décrire le schéma d'authentification qui permet aux utilisateurs de se connecter une seule fois pour accéder à plusieurs applications et sites Web.

Fonctionnalités de l'IAM Identity Center

IAM Identity Center inclut les fonctionnalités et fonctionnalités de base suivantes :

Gérez les identités du personnel

Les utilisateurs humains qui créent ou exploitent des charges de travail AWS sont également appelés utilisateurs du personnel ou identités du personnel. Les utilisateurs du personnel sont des employés ou des sous-traitants auxquels vous autorisez l'accès Comptes AWS au sein de votre organisation et à vos applications métier internes. Ces personnes peuvent être des développeurs qui créent vos systèmes internes et destinés aux clients, ou des utilisateurs de systèmes de base de données et d'applications internes. Vous pouvez créer des utilisateurs et des groupes d'employés dans IAM Identity Center, ou vous connecter et synchroniser avec un ensemble existant d'utilisateurs et de groupes dans votre propre source d'identité pour une utilisation dans toutes vos applications Comptes AWS et applications. Pour plus d'informations, consultez Gérez votre source d'identité.

Gérer les instances d'IAM Identity Center

IAM Identity Center prend en charge deux types d'instances : les instances d'organisation et les instances de compte. Une instance d'organisation est la meilleure pratique. C'est la seule instance qui vous permet de gérer l'accès aux applications Comptes AWS et elle est recommandée pour toutes les utilisations en production des applications. Une instance d'organisation est déployée dans le compte AWS Organizations de gestion et vous fournit un point unique à partir duquel vous pouvez gérer l'accès des utilisateurs dans l' AWS environnement.

Les instances de compte sont liées à Compte AWS celles dans lesquelles elles sont activées. Utilisez les instances de compte d'IAM Identity Center uniquement pour prendre en charge les déploiements isolés de certaines applications AWS gérées. Pour plus d'informations, consultez Gérer les instances d'organisation et de compte d'IAM Identity Center.

Gérez l'accès à plusieurs Comptes AWS

Avec les autorisations multicomptes, vous pouvez planifier et mettre en œuvre de manière centralisée des autorisations pour plusieurs comptes Comptes AWS à la fois sans avoir à configurer manuellement chacun de vos comptes. Vous pouvez créer des autorisations basées sur des fonctions professionnelles courantes ou définir des autorisations personnalisées répondant à vos besoins en matière de sécurité. Vous pouvez ensuite attribuer ces autorisations aux utilisateurs du personnel afin de contrôler leur accès à des comptes spécifiques.

Cette fonctionnalité optionnelle n'est disponible que pour les instances d'organisation. Si vous utilisez la gestion des rôles IAM par compte dans votre environnement, les deux systèmes peuvent coexister. Si vous souhaitez essayer les autorisations multi-comptes, vous pouvez commencer par implémenter ce système de manière limitée et migrer une plus grande partie de votre environnement pour utiliser ce système au fil du temps.

Gérez l'accès aux applications

IAM Identity Center vous permet de simplifier la gestion de l'accès aux applications. Avec IAM Identity Center, vous pouvez accorder aux utilisateurs de votre personnel d'IAM Identity Center un accès par authentification unique aux applications.

AWS applications gérées

AWS fournit des applications telles qu' Amazon Redshift Amazon Managed Grafana et Amazon Monitron, qui s'intègrent à IAM Identity Center. Ces applications peuvent utiliser IAM Identity Center pour l'authentification, les services d'annuaire et la propagation d'identités fiables. Vos utilisateurs bénéficient d'une expérience d'authentification unique cohérente, et

comme les applications partagent une vision commune des utilisateurs, des groupes et de l'appartenance aux groupes, les utilisateurs bénéficient également d'une expérience cohérente lorsqu'ils partagent les ressources de l'application avec d'autres utilisateurs. Vous pouvez configurer des applications AWS gérées pour qu'elles fonctionnent avec IAM Identity Center directement depuis les consoles d'applications pertinentes ou via les API.

Applications gérées par le client

Dans IAM Identity Center, vous pouvez accorder aux utilisateurs de votre personnel un accès par authentification unique aux applications qui prennent en charge la fédération des identités avec SAML 2.0. De nombreuses applications SAML 2.0 couramment utilisées, telles que Salesforce et Microsoft 365, fonctionnent avec IAM Identity Center et sont disponibles dans le catalogue d'applications de la console IAM Identity Center. Il s'agit d'une fonctionnalité facultative qui peut être utile si vous utilisez de telles applications et si vous créez vos utilisateurs et groupes dans IAM Identity Center, ou si vous utilisez le service de domaine Microsoft Active Directory comme source d'identité.

Propagation d’identité approuvée entre applications

La propagation fiable des identités fournit une expérience d'authentification unique rationalisée aux utilisateurs d'outils de requête et d'applications de business intelligence (BI) qui ont besoin d'accéder aux données des AWS services. La gestion de l'accès aux données est basée sur l'identité de l'utilisateur, de sorte que les administrateurs peuvent accorder l'accès en fonction de l'appartenance des utilisateurs et des groupes aux utilisateurs existants. L'accès des utilisateurs aux AWS services et aux autres événements est enregistré dans des journaux et des CloudTrail événements spécifiques aux services, afin que les auditeurs sachent quelles actions les utilisateurs ont entreprises et à quelles ressources ils ont accédé.

AWS accès au portail pour vos utilisateurs

Le portail AWS d'accès est un portail Web simple qui fournit à vos utilisateurs un accès fluide à toutes les applications qui leur sont Comptes AWS assignées.

Renommer le centre d'identité IAM

Le 26 juillet 2022, AWS Single Sign-On a été renommé en AWS IAM Identity Center. Pour les clients existants, le tableau suivant est destiné à décrire certains des changements de termes les plus courants qui ont été mis à jour dans ce guide à la suite du changement de nom.

Terme d'héritage	Mandat en cours
AWS Utilisateur SSO ou utilisateur SSO	utilisateur du personnel ou utilisateur
AWS Portail utilisateur SSO ou portail utilisateur	AWS portail d'accès
AWS Applications intégrées au SSO	AWS applications gérées
AWS Annuaire SSO	Répertoire d'Identity Center
AWS Boutique SSO ou boutique d' AWS identité SSO	magasin d'identité utilisé par IAM Identity Center

Le tableau suivant décrit les modifications de nom applicables aux utilisateurs, aux développeurs et au guide de référence des API qui ont également eu lieu à la suite de ce changement de nom.

Guide de l'héritage	Guide actuel
AWS Guide de l'utilisateur avec authentification unique	Guide de l'utilisateur d'IAM Identity Center
AWS Guide du développeur de mise en œuvre de l'authentification unique SCIM	Guide du développeur de mise en œuvre d'IAM Identity Center SCIM
AWS Guide de référence de l'API d'authentification unique	Référence de l'API IAM Identity Center
AWS Guide de référence de l'API Single Sign-On Identity Store	Référence de l'API Identity Store
AWS Guide de référence de l'API OIDC à connexion unique	Référence de l'API OIDC d'IAM Identity Center
AWS Guide de référence de l'API du portail d'authentification unique	Référence de l'API du portail IAM Identity Center

Les anciens espaces de noms restent les mêmes

Les espaces de noms `sso` et `identitystore` API ainsi que les espaces de noms associés suivants restent inchangés à des fins de rétrocompatibilité.

- Commandes CLI
  - `aws configure sso`
  - `identitystore`
  - `sso`
  - `sso-admin`
  - `sso-oidc`
- Politiques gérées contenant `AWSSSO` des `AWSIdentitySync` préfixes
- Points de terminaison de service contenant `sso` et `identitystore`
- AWS CloudFormationressources contenant des `AWS::SSO` préfixes
- Rôle lié à un service contenant `AWSServiceRoleForSSO`
- URL de console contenant `sso` et `singlesignon`
- URL de documentation contenant `singlesignon`

Activant AWS IAM Identity Center

Procédez comme suit pour vous connecter AWS Management Console et activer une instance d'organisation d'IAM Identity Center.

1. Procédez de l'une des manières suivantes pour vous connecter au AWS Management Console.
   - Nouvel utilisateur AWS (utilisateur root) : connectez-vous en tant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.
   - Vous utilisez déjà AWS (informations d'identification IAM) : connectez-vous à l'aide de vos informations d'identification IAM avec des autorisations administratives.
2. Ouvrez la console IAM Identity Center.
3. Sous Activer le centre d'identité IAM, sélectionnez Activer avec AWS Organizations.
4. Facultatif Ajoutez les balises que vous souhaitez associer à cette instance d'organisation.
5. Facultatif Configurer l'administration déléguée.

> **Note**
>
> Si vous utilisez un environnement multi-comptes, nous vous recommandons de configurer l'administration déléguée. Grâce à l'administration déléguée, vous pouvez limiter le nombre de personnes ayant besoin d'accéder au compte de gestion dans AWS Organizations. Pour plus d'informations, consultez Administration déléguée.

> **Important**
>
> La possibilité de créer des instances de compte d'IAM Identity Center est activée par défaut. Les instances de compte d'IAM Identity Center incluent un sous-ensemble de fonctionnalités disponibles pour une instance d'organisation. Vous pouvez contrôler si les utilisateurs peuvent accéder à cette fonctionnalité à l'aide d'une politique de contrôle des services.

Devez-vous mettre à jour les pare-feux et les passerelles ?

Si vous filtrez l'accès à des AWS domaines ou points de terminaison d'URL spécifiques à l'aide d'une solution de filtrage de contenu Web telle que les pare-feux de nouvelle génération (NGFW) ou les passerelles Web sécurisées (SWG), vous devez ajouter les domaines ou points de terminaison d'URL suivants aux listes d'autorisation de votre solution de filtrage de contenu Web. Cela vous permet d'accéder à votre portail AWS d'accès.

- *[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

Considérations relatives à l'autorisation de répertorier des domaines et des points de terminaison d'URL

Comprenez l'impact de l'autorisation de répertorier des domaines au-delà du portail AWS d'accès.

- Pour accéder à Comptes AWS AWS Management Console, et à la console IAM Identity Center depuis votre portail d' AWS accès, vous devez autoriser des domaines supplémentaires sur la liste. Reportez-vous à la section Résolution des problèmes du Guide de démarrage pour AWS Management Console obtenir la liste des AWS Management Console domaines.
- Pour accéder aux applications AWS gérées depuis votre portail AWS d'accès, vous devez autoriser leurs domaines respectifs à les répertorier. Reportez-vous à la documentation de service correspondante pour obtenir des conseils.

- Ces listes d'autorisation couvrent les AWS services. Si vous utilisez un logiciel externe, tel qu'un logiciel externe IdPs (par exemple, Okta etMicrosoft Entra ID), vous devez inclure leurs domaines dans vos listes d'autorisation.

Vous êtes maintenant prêt à configurer IAM Identity Center. Lorsque vous activez IAM Identity Center, il est automatiquement configuré avec un répertoire Identity Center comme source d'identité par défaut, ce qui constitue le moyen le plus rapide de commencer à utiliser IAM Identity Center. Pour obtenir des instructions, veuillez consulter Configuration de l'accès utilisateur avec le répertoire IAM Identity Center par défaut.

Si vous souhaitez en savoir plus sur le fonctionnement d'IAM Identity Center avec les Organizations, les sources d'identité et les rôles IAM, consultez les rubriques suivantes.

Rubriques

Prérequis et considérations

Les rubriques suivantes fournissent des informations sur les conditions préalables et d'autres considérations relatives à la configuration d'IAM Identity Center.

Considérations relatives au choix d'un Région AWS

Vous pouvez activer une instance IAM Identity Center dans une instance unique prise en charge Région AWS de votre choix. Le choix d'une région nécessite une évaluation de vos priorités en fonction de vos cas d'utilisation et des politiques de l'entreprise. L'accès à votre IAM Identity Center Comptes AWS et aux applications cloud depuis celui-ci ne dépend pas de ce choix ; toutefois, l'accès aux applications AWS gérées et la possibilité de les utiliser AWS Managed Microsoft AD comme source d'identité peuvent dépendre de ce choix. Reportez-vous aux points de terminaison et quotas AWS IAM Identity Center dans le Références générales AWS pour obtenir la liste des régions prises en charge par IAM Identity Center.

Considérations clés pour le choix d'un Région AWS.

- Emplacement géographique — Lorsque vous sélectionnez la région la plus proche géographiquement de la majorité de vos utilisateurs finaux, ils bénéficieront d'une latence d'accès

plus faible au portail AWS d'accès et aux applications AWS gérées, telles qu'Amazon SageMaker Studio.

- Disponibilité des applications AWS gérées : les applications AWS gérées, telles qu'Amazon SageMaker, ne peuvent fonctionner que dans les conditions Régions AWS qu'elles prennent en charge. Activez le centre d'identité IAM dans une région prise en charge par les applications AWS gérées que vous souhaitez utiliser avec celui-ci. De nombreuses applications AWS gérées peuvent également fonctionner uniquement dans la région où vous avez activé IAM Identity Center.
- Souveraineté numérique — Les réglementations en matière de souveraineté numérique ou les politiques de l'entreprise peuvent imposer l'utilisation d'un élément particulier Région AWS. Consultez le service juridique de votre entreprise.
- Source d'identité : si vous utilisez AD AWS Managed Microsoft AD Connector comme source d'identité, sa région d'origine doit correspondre à celle Région AWS dans laquelle vous avez activé IAM Identity Center.
- Régions désactivées par défaut : AWS à l'origine, toutes les nouvelles Régions AWS étaient activées pour être utilisées Comptes AWS par défaut, ce qui permettait automatiquement à vos utilisateurs de créer des ressources dans n'importe quelle région. Désormais, lors de l' AWS ajout d'une nouvelle région, son utilisation est désactivée par défaut dans tous les comptes. Si vous déployez IAM Identity Center dans une région désactivée par défaut, vous devez activer cette région dans tous les comptes pour lesquels vous souhaitez gérer l'accès à IAM Identity Center. Cela est nécessaire même si vous ne prévoyez pas de créer de ressources dans cette région dans ces comptes.

  Vous pouvez activer une région pour les comptes courants de votre organisation et vous devez répéter cette action pour les nouveaux comptes que vous pourriez ajouter ultérieurement. Pour obtenir des instructions, voir Activer ou désactiver une région dans votre organisation dans le guide de AWS Organizations l'utilisateur. Pour éviter de répéter ces étapes supplémentaires, vous pouvez choisir de déployer votre IAM Identity Center dans une région activée par défaut. À titre de référence, les régions suivantes sont activées par défaut :

  - USA Est (Ohio)
  - USA Est (Virginie du Nord)
  - USA Ouest (Oregon)
  - USA Ouest (Californie du Nord)
  - Europe (Paris)
  - Amérique du Sud (São Paulo)
  - Asie-Pacifique (Mumbai)

- Europe (Stockholm)
- Asie-Pacifique (Séoul)
- Asie Pacifique (Tokyo)
- Europe (Irlande)
- Europe (Francfort)
- Europe (Londres)
- Asie-Pacifique (Singapour)
- Asie-Pacifique (Sydney)
- Canada (Centre)
- Asie-Pacifique (Osaka)

- Appels interrégionaux : dans certaines régions, IAM Identity Center peut appeler Amazon Simple Email Service dans une autre région pour envoyer un e-mail. Lors de ces appels interrégionaux, le centre d'identité IAM envoie certains attributs utilisateur à l'autre région. Pour plus d'informations sur les régions, consultez AWS IAM Identity Center Disponibilité de la région.

Commutation Régions AWS

Vous pouvez changer de région de centre d'identité IAM uniquement en supprimant l'instance actuelle et en créant une nouvelle instance dans une autre région. Si vous avez déjà activé une application AWS gérée avec votre instance existante, vous devez d'abord la supprimer avant de supprimer votre IAM Identity Center. Vous devez recréer les utilisateurs, les groupes, les ensembles d'autorisations, les applications et les attributions dans la nouvelle instance. Vous pouvez utiliser le compte IAM Identity Center et les API d'attribution d'applications pour obtenir un instantané de votre configuration, puis utiliser cet instantané pour reconstruire votre configuration dans une nouvelle région. Vous devrez peut-être également recréer une configuration d'IAM Identity Center via la console de gestion de votre nouvelle instance. Pour obtenir des instructions sur la suppression d'IAM Identity Center, consultezSupprimer la configuration de votre IAM Identity Center.

Quota pour les rôles IAM créés par IAM Identity Center

IAM Identity Center crée des rôles IAM pour autoriser les utilisateurs à accéder aux ressources. Lorsque vous attribuez un ensemble d'autorisations, IAM Identity Center crée les rôles IAM contrôlés par IAM Identity Center correspondants dans chaque compte et associe les politiques spécifiées dans le jeu d'autorisations à ces rôles. IAM Identity Center gère le rôle et permet aux utilisateurs autorisés que vous avez définis d'assumer le rôle, en utilisant le portail d' AWS accès ou. AWS CLI Lorsque

vous modifiez l'ensemble d'autorisations, IAM Identity Center veille à ce que les politiques et rôles IAM correspondants soient mis à jour en conséquence.

Si vous avez déjà configuré des rôles IAM dans votre compte Compte AWS, nous vous recommandons de vérifier si votre compte atteint le quota de rôles IAM. Le quota par défaut de rôles IAM par compte est de 1 000 rôles. Pour plus d'informations, consultez la section Quotas d'objets IAM.

Si vous approchez du quota, pensez à demander une augmentation du quota. Sinon, vous risquez de rencontrer des problèmes avec IAM Identity Center lorsque vous attribuez des ensembles d'autorisations à des comptes qui ont dépassé le quota de rôles IAM. Pour plus d'informations sur la procédure à suivre pour demander une augmentation de quota, voir Demande d'augmentation de quota dans le Guide de l'utilisateur du Service Quotas.

> **Note**
>
> Si vous passez en revue les rôles IAM dans un compte qui utilise déjà IAM Identity Center, vous remarquerez peut-être que les noms de rôles commencent par. “AWSReservedSSO_” Il s'agit des rôles que le service IAM Identity Center a créés dans le compte, et ils proviennent de l'attribution d'un ensemble d'autorisations au compte.

IAM Identity Center et AWS Organizations

AWS Organizations est recommandé, mais non obligatoire, pour une utilisation avec IAM Identity Center. Si vous n'avez pas créé d'organisation, vous n'êtes pas obligé de le faire. Lorsque vous activez IAM Identity Center, vous devez choisir d'activer ou non le service avec AWS Organizations. Lorsque vous configurez une organisation, le Compte AWS compte de gestion de l'organisation devient le compte de gestion de l'organisation. L'utilisateur root du Compte AWS est désormais le propriétaire du compte de gestion de l'organisation. Tout compte supplémentaire Comptes AWS que vous invitez à rejoindre votre organisation est considéré comme un compte de membre. Le compte de gestion crée les ressources, les unités organisationnelles et les politiques de l'organisation qui gèrent les comptes des membres. Les autorisations sont déléguées aux comptes des membres par le compte de gestion.

> **Note**
>
> Nous vous recommandons d'activer IAM Identity Center avec AWS Organizations, ce qui crée une instance organisationnelle d'IAM Identity Center. Une instance d'organisation est

notre meilleure pratique recommandée, car elle prend en charge toutes les fonctionnalités d'IAM Identity Center et fournit des fonctionnalités de gestion centralisée. Pour plus d'informations, consultez Gérer les instances d'organisation et de compte d'IAM Identity Center.

Si vous avez déjà configuré AWS Organizations et que vous comptez ajouter IAM Identity Center à votre organisation, assurez-vous que toutes les AWS Organizations fonctionnalités sont activées. Lorsque vous créez une organisation, toutes les fonctions sont activées par défaut. Pour de plus amples informations, consultez Activation de toutes les fonctionnalités de l'organisation dans le Guide de l'utilisateur AWS Organizations .

Pour activer IAM Identity Center, vous devez vous connecter au en vous AWS Management Console connectant à votre compte de AWS Organizations gestion en tant qu'utilisateur disposant d'informations d'identification administratives ou en tant qu'utilisateur root (ce n'est pas recommandé, sauf s'il n'existe aucun autre utilisateur administratif). Vous ne pouvez pas activer IAM Identity Center lorsque vous êtes connecté avec les informations d'identification administratives d'un compte AWS Organizations membre. Pour plus d'informations, consultez la section Création et gestion d'une AWS organisation dans le guide de AWS Organizations l'utilisateur.

Confirmez vos sources d'identité dans IAM Identity Center

Votre source d'identité dans IAM Identity Center définit l'endroit où vos utilisateurs et vos groupes sont gérés. Après avoir activé IAM Identity Center, vérifiez que vous utilisez la source d'identité de votre choix.

Confirmez votre source d'identité

1. Ouvrez la console IAM Identity Center.
2. Sur la page du tableau de bord, sous la section Étapes de configuration recommandées, choisissez Confirmer votre source d'identité. Vous pouvez également accéder à cette page en choisissant Paramètres et en choisissant l'onglet Source d'identité.
3. Aucune action n'est nécessaire si vous souhaitez conserver la source d'identité qui vous a été attribuée. Si vous préférez le modifier, choisissez Actions, puis Change identity source.

   Vous pouvez choisir l'une des sources d'identité suivantes :

Répertoire d'Identity Center

Lorsque vous activez IAM Identity Center pour la première fois, il est automatiquement configuré avec un répertoire Identity Center comme source d'identité par défaut. Si vous n'utilisez pas encore un autre fournisseur d'identité externe, vous pouvez commencer à créer vos utilisateurs et groupes, et attribuer leur niveau d'accès à vos applications Comptes AWS et à vos applications. Pour un didacticiel sur l'utilisation de cette source d'identité, consultezConfiguration de l'accès utilisateur avec le répertoire IAM Identity Center par défaut.

Active Directory

Si vous gérez déjà des utilisateurs et des groupes dans votre AWS Managed Microsoft AD annuaire en utilisant AWS Directory Service ou dans votre annuaire autogéréActive Directory (AD), nous vous recommandons de connecter cet annuaire lorsque vous activez IAM Identity Center. Ne créez aucun utilisateur ni groupe dans le répertoire par défaut d'Identity Center. IAM Identity Center utilise la connexion fournie par le AWS Directory Service pour synchroniser les informations relatives aux utilisateurs, aux groupes et aux membres entre votre répertoire source dans Active Directory et le magasin d'identités IAM Identity Center. Pour plus d'informations, consultez Se connecter à un Microsoft AD annuaire.

> **Note**
>
> IAM Identity Center ne prend pas en charge Simple AD basé sur Samba4 en tant que source d'identité.

Fournisseur d'identité externe

Pour les fournisseurs d'identité externes (IdPs) tels que Okta ouMicrosoft Entra ID, vous pouvez utiliser IAM Identity Center pour authentifier les identités IdPs via la norme SAML (Security Assertion Markup Language) 2.0. Le protocole SAML ne permet pas d'interroger l'IdP pour en savoir plus sur les utilisateurs et les groupes. Vous informez IAM Identity Center de l'existence de ces utilisateurs et groupes en les configurant dans IAM Identity Center. Vous pouvez effectuer le provisionnement automatique (synchronisation) des informations sur les utilisateurs et les groupes depuis votre IdP vers IAM Identity Center à l'aide du protocole System for Cross-domain Identity Management (SCIM) v2.0 si votre IdP prend en charge le SCIM. Sinon, vous pouvez configurer manuellement vos utilisateurs et vos groupes

en saisissant manuellement les noms d'utilisateur, les adresses e-mail et les groupes dans IAM Identity Center.

Pour obtenir des instructions détaillées sur la configuration de votre source d'identité, consultezTutoriels de mise en route.

> **Note**
>
> Si vous envisagez d'utiliser un fournisseur d'identité externe, notez que c'est l'IdP externe, et non le IAM Identity Center, qui gère les paramètres d'authentification multifactorielle (MFA). L'authentification MFA dans IAM Identity Center n'est pas prise en charge pour une utilisation par des utilisateurs externes. IdPs Pour plus d'informations, consultez Inviter les utilisateurs à utiliser le MFA.

La source d'identité que vous choisissez détermine où IAM Identity Center recherche les utilisateurs et les groupes ayant besoin d'un accès par authentification unique. Après avoir confirmé ou modifié votre source d'identité, vous allez créer ou spécifier un utilisateur et lui attribuer des autorisations administratives à votre Compte AWS.

> **Important**
>
> Si vous gérez déjà des utilisateurs et des groupes dans un fournisseur d'identité (IdP) externe Active Directory ou dans un fournisseur d'identité externe, nous vous recommandons d'envisager de connecter cette source d'identité lorsque vous activez IAM Identity Center et que vous choisissez votre source d'identité. Cela doit être fait avant de créer des utilisateurs et des groupes dans le répertoire par défaut d'Identity Center et d'effectuer des assignations. Si vous gérez déjà des utilisateurs et des groupes dans une source d'identité dans IAM Identity Center, le passage à une autre source d'identité peut supprimer toutes les attributions d'utilisateurs et de groupes que vous avez configurées dans IAM Identity Center. Dans ce cas, tous les utilisateurs, y compris l'utilisateur administratif d'IAM Identity Center, perdront l'accès par authentification unique à leurs applications Comptes AWS et à leurs applications. Pour plus d'informations, consultez Considérations relatives à la modification de votre source d'identité.

Après avoir configuré votre source d'identité, vous pouvez rechercher des utilisateurs ou des groupes pour leur accorder un accès par authentification unique aux applications cloud Comptes AWS, ou aux deux.

Tutoriels de mise en route

Vous pouvez avoir une source d'identité par organisation. Il est donc important de prendre le temps de tester les fonctionnalités de chacune d'entre elles.

Dans cette section, vous pouvez choisir l'un des didacticiels suivants pour configurer IAM Identity Center avec votre source d'identité préférée, créer un utilisateur administratif et configurer des ensembles d'autorisations pour permettre à vos utilisateurs d'accéder aux ressources.

Avant de commencer l'un de ces didacticiels, activez IAM Identity Center. Pour plus d'informations, consultez Activant AWS IAM Identity Center.

Rubriques

- Configuration de l'accès utilisateur avec le répertoire IAM Identity Center par défaut
- Utilisation d'Active Directory comme source d'identité
- Setting up SCIM provisioning between CyberArk and IAM Identity Center
- Configurer SAML et SCIM avec un IAM Google Workspace Identity Center
- Utilisation d'IAM Identity Center pour vous connecter à votre plateforme d'JumpCloudannuaire
- Configurer SAML et SCIM avec un IAM Microsoft Entra ID Identity Center
- Configurer SAML et SCIM avec un IAM Okta Identity Center
- Configuration du provisionnement SCIM entre OneLogin et IAM Identity Center
- Utilisation de Ping Identity produits avec IAM Identity Center

Configuration de l'accès utilisateur avec le répertoire IAM Identity Center par défaut

Lorsque vous activez IAM Identity Center pour la première fois, il est automatiquement configuré avec un répertoire Identity Center comme source d'identité par défaut. Vous n'avez donc pas besoin de choisir une source d'identité. Si votre organisation utilise un autre fournisseur d'identité tel que AWS Directory Service for Microsoft Active DirectoryMicrosoft Entra ID, ou Okta envisagez d'intégrer cette source d'identité à IAM Identity Center au lieu d'utiliser la configuration par défaut.

Objectif

Dans ce didacticiel, vous allez utiliser le répertoire par défaut comme source d'identité et configurer et tester l'accès des utilisateurs. Dans ce scénario, vous gérez tous les utilisateurs et groupes dans IAM Identity Center. Les utilisateurs se connectent via le portail AWS d'accès. Ce didacticiel est destiné aux utilisateurs qui découvrent AWS ou utilisent déjà IAM pour gérer des utilisateurs et des groupes. Au cours des prochaines étapes, vous allez créer les éléments suivants :

- Une utilisatrice administrative nommée *Nikki Wolf*
- Un groupe nommé *Admin team*
- Un ensemble d'autorisations nommé *AdminAccess*

Pour vérifier que tout a été créé correctement, vous devez vous connecter et définir le mot de passe de l'utilisateur administratif. Après avoir terminé ce didacticiel, vous pouvez utiliser l'utilisateur administratif pour ajouter d'autres utilisateurs dans IAM Identity Center, créer des ensembles d'autorisations supplémentaires et configurer l'accès organisationnel aux applications.

Si vous n'avez pas encore activé IAM Identity Center, consultezActivant AWS IAM Identity Center.

Avant de commencer :

Procédez de l'une des manières suivantes pour vous connecter au AWS Management Console.

- Nouvel utilisateur AWS (utilisateur root) : connectez-vous en tant que propriétaire du compte en choisissant l'utilisateur Compte AWS root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.
- Vous utilisez déjà AWS (informations d'identification IAM) : connectez-vous à l'aide de vos informations d'identification IAM avec des autorisations administratives.

Ouvrez la console IAM Identity Center.

Étape 1 : ajouter un utilisateur

1. Dans le volet de navigation d'IAM Identity Center, choisissez Utilisateurs, puis sélectionnez Ajouter un utilisateur.
2. Sur la page Spécifier les détails de l'utilisateur, complétez les informations suivantes :
    - Nom d'utilisateur - Pour ce didacticiel, entrez *nikkiw*.

Lorsque vous créez des utilisateurs, choisissez des noms d'utilisateur faciles à mémoriser. Vos utilisateurs doivent mémoriser leur nom d'utilisateur pour se connecter au portail AWS d'accès et vous ne pourrez pas le modifier ultérieurement.

- Mot de passe - Choisissez Envoyer un e-mail à cet utilisateur avec les instructions de configuration du mot de passe (recommandé).

  Cette option envoie à l'utilisateur une adresse e-mail provenant d'Amazon Web Services, avec comme objet Invitation à rejoindre IAM Identity Center (successeur de Single Sign-On). AWS L'e-mail provient de l'un `no-reply@signin.aws` ou de `no-reply@login.awsapps.com`. Ajoutez ces adresses e-mail à votre liste d'expéditeurs approuvés.
- Adresse e-mail - Entrez l'adresse e-mail de l'utilisateur à laquelle vous pouvez recevoir l'e-mail. Ensuite, saisissez-le à nouveau pour le confirmer. Chaque utilisateur doit avoir une adresse e-mail unique.
- Prénom - Entrez le prénom de l'utilisateur. Pour ce tutoriel, entrez *`Nikki`*.
- Nom de famille - Entrez le nom de famille de l'utilisateur. Pour ce didacticiel, entrez *`Wolf`*.
- Nom d'affichage : la valeur par défaut est le prénom et le nom de famille de l'utilisateur. Si vous souhaitez modifier le nom d'affichage, vous pouvez saisir un autre nom. Le nom d'affichage est visible dans le portail de connexion et dans la liste des utilisateurs.
- Complétez les informations facultatives si vous le souhaitez. Il n'est pas utilisé pendant ce didacticiel et vous pourrez le modifier ultérieurement.

3. Choisissez Suivant. La page Ajouter un utilisateur aux groupes apparaît. Nous allons créer un groupe auquel attribuer des autorisations administratives au lieu de les donner directement à *`Nikki`*.

   Choisissez Créer un groupe

   Un nouvel onglet de navigateur s'ouvre pour afficher la page Créer un groupe.

   a. Sous Détails du groupe, dans Nom du groupe, entrez le nom du groupe. Nous recommandons un nom de groupe qui identifie le rôle du groupe. Pour ce didacticiel, entrez *`Admin team`*.

   b. Choisissez Créer un groupe

   c. Fermez l'onglet du navigateur de groupes pour revenir à l'onglet du navigateur Ajouter un utilisateur.

4. Dans la zone Groupes, sélectionnez le bouton Actualiser. Le groupe de *l'équipe d'administrateurs* apparaît dans la liste.

   Cochez la case à côté de *l'équipe d'administration*, puis choisissez Suivant.

5. Sur la page Vérifier et ajouter un utilisateur, confirmez les points suivants :

   - Les informations principales apparaissent comme vous le souhaitiez
   - Groupes affiche l'utilisateur ajouté au groupe que vous avez créé

   Si vous souhaitez apporter des modifications, choisissez Modifier. Lorsque tous les détails sont corrects, choisissez Ajouter un utilisateur.

   Un message de notification vous informe que l'utilisateur a été ajouté.

Ensuite, vous allez ajouter des autorisations administratives pour le groupe *d'équipe d'administration* afin que *Nikki* ait accès aux ressources.

Étape 2 : ajouter des autorisations administratives

1. Dans le volet de navigation d'IAM Identity Center, sous Autorisations multi-comptes, sélectionnez. Comptes AWS
2. Sur la Comptes AWSpage, la structure organisationnelle affiche votre organisation avec vos comptes situés en dessous dans la hiérarchie. Cochez la case correspondant à votre compte de gestion, puis sélectionnez Attribuer des utilisateurs ou des groupes.
3. Le flux de travail Attribuer des utilisateurs et des groupes s'affiche. Il se compose de trois étapes :

   a. Pour l'étape 1 : Sélectionnez les utilisateurs et les groupes, choisissez le groupe *d'équipe d'administrateurs* que vous avez créé. Ensuite, sélectionnez Suivant.

   b. Pour l'étape 2 : Sélectionnez des ensembles d'autorisations, choisissez Créer un ensemble d'autorisations pour ouvrir un nouvel onglet qui vous indique les trois sous-étapes nécessaires à la création d'un ensemble d'autorisations.

      i. Pour l'étape 1 : Sélectionnez le type d'ensemble d'autorisations, procédez comme suit :

         - Dans Type d'ensemble d'autorisations, choisissez Ensemble d'autorisations prédéfini.

- Dans Politique pour un ensemble d'autorisations prédéfini, sélectionnez AdministratorAccess.

Choisissez Suivant.

ii. Pour l'étape 2 : Spécifiez les détails de l'ensemble d'autorisations, conservez les paramètres par défaut et choisissez Next.

Les paramètres par défaut créent un ensemble d'autorisations nommé *`AdministratorAccess`*avec une durée de session fixée à une heure. Vous pouvez modifier le nom de l'ensemble d'autorisations en saisissant un nouveau nom dans le champ Nom de l'ensemble d'autorisations.

iii. Pour l'étape 3 : révision et création, vérifiez que le type d'ensemble d'autorisations utilise la politique AWS gérée AdministratorAccess. Choisissez Créer. Sur la page Ensembles d'autorisations, une notification apparaît pour vous informer que l'ensemble d'autorisations a été créé. Vous pouvez maintenant fermer cet onglet dans votre navigateur Web.

Dans l'onglet du navigateur Attribuer des utilisateurs et des groupes, vous êtes toujours à l'étape 2 : Sélectionnez les ensembles d'autorisations à partir desquels vous avez lancé le flux de travail de création d'ensembles d'autorisations.

Dans la zone Ensembles d'autorisations, cliquez sur le bouton Actualiser. L'ensemble *`AdministratorAccess`*d'autorisations que vous avez créé apparaît dans la liste. Cochez la case correspondant à cet ensemble d'autorisations, puis choisissez Next.

c. Sur la page Étape 3 : Révision et envoi des tâches, vérifiez que le groupe *`d'équipes d'administrateurs`* est sélectionné et que l'ensemble d'*`AdministratorAccess`*autorisations est sélectionné, puis choisissez Soumettre.

La page Compte AWS est mise à jour avec un message indiquant que vous êtes en cours de configuration. Patientez jusqu'à ce que le processus soit terminé.

Vous êtes renvoyé à la Comptes AWS page. Un message de notification vous informe que votre Compte AWS compte a été réapprovisionné et que l'ensemble d'autorisations mis à jour a été appliqué.

> **Félicitations !**
>
> Vous avez correctement configuré votre premier utilisateur, votre premier groupe et votre premier ensemble d'autorisations.

Dans la partie suivante de ce didacticiel, vous testerez l'accès *de Nikki* en vous connectant au portail d' AWS accès avec ses informations d'identification administratives et en définissant son mot de passe. Déconnectez-vous de la console maintenant.

Étape 3 : Tester l'accès utilisateur

Maintenant que *Nikki Wolf* est une utilisatrice de votre organisation, elle peut se connecter et accéder aux ressources auxquelles elle est autorisée conformément à son ensemble d'autorisations. Pour vérifier que l'utilisateur est correctement configuré, à l'étape suivante, vous utiliserez les informations d'identification *de Nikki* pour vous connecter et configurer son mot de passe. Lorsque vous avez ajouté l'utilisateur *Nikki Wolf* à l'étape 1, vous avez choisi de faire en sorte que *Nikki* reçoive un e-mail contenant les instructions de configuration du mot de passe. Il est temps d'ouvrir cet e-mail et de procéder comme suit :

1. Dans l'e-mail, sélectionnez le lien Accepter l'invitation pour accepter l'invitation.

   > **Note**
   >
   > L'e-mail inclut également le nom d'utilisateur *de Nikki* et l'URL du portail d' AWS accès qu'ils utiliseront pour se connecter à l'organisation. Enregistrez ces informations pour une utilisation future.

   Vous êtes redirigé vers la page d'inscription d'un nouvel utilisateur où vous pouvez définir le mot *de passe de Nikki*.

2. Après avoir défini le mot *de passe de Nikki*, vous êtes dirigé vers la page de connexion. Entrez ***nikkiw*** et choisissez Suivant, puis entrez le mot de passe ***de Nikki*** et choisissez Se connecter.
3. Le portail AWS d'accès s'ouvre et affiche l'organisation et les applications auxquelles vous pouvez accéder.

Sélectionnez l'organisation pour la développer dans une liste Comptes AWS , puis sélectionnez le compte pour afficher les rôles que vous pouvez utiliser pour accéder aux ressources du compte.

Chaque ensemble d'autorisations comporte deux méthodes de gestion que vous pouvez utiliser, soit les clés de rôle, soit les clés d'accès.

- Rôle, par exemple *`AdministratorAccess`*- Ouvre le AWS Console Home.
- Clés d'accès : fournit des informations d'identification que vous pouvez utiliser avec le AWS CLI ou le AWS SDK. Inclut les informations relatives à l'utilisation d'informations d'identification à court terme actualisées automatiquement ou de clés d'accès à court terme. Pour plus d'informations, consultez Obtention des informations d'identification utilisateur d'IAM Identity Center pour les SDK AWS CLI ou AWS.

4. Cliquez sur le lien Rôle pour vous connecter au AWS Console Home.

Vous êtes connecté et vous avez accédé à la AWS Console Home page. Explorez la console et confirmez que vous disposez de l'accès attendu.

Étapes suivantes

Maintenant que vous avez créé un utilisateur administratif dans IAM Identity Center, vous pouvez :

- Attribuer des applications
- Ajouter d'autres utilisateurs
- Attribuer des utilisateurs à des comptes
- Configurer des ensembles d'autorisations supplémentaires

> **Note**
>
> Vous pouvez attribuer plusieurs ensembles d'autorisations au même utilisateur. Pour suivre la meilleure pratique consistant à appliquer des autorisations de moindre privilège, après avoir créé votre utilisateur administratif, créez un ensemble d'autorisations plus restrictif et attribuez-le au même utilisateur. Ainsi, vous pouvez accéder à votre compte uniquement Compte AWS avec les autorisations dont vous avez besoin, plutôt qu'avec des autorisations administratives.

Une fois que vos utilisateurs ont accepté leur invitation à activer leur compte et qu'ils se sont connectés au portail d' AWS accès, les seuls éléments qui apparaissent dans le Comptes AWS portail concernent les rôles et les applications auxquels ils sont affectés.

> **Important**
>
> Nous vous recommandons vivement d'activer l'authentification multifactorielle (MFA) pour vos utilisateurs. Pour plus d'informations, voir Authentification multifactorielle pour les utilisateurs d'Identity Center.

Utilisation d'Active Directory comme source d'identité

Si vous gérez les utilisateurs de votre AWS Managed Microsoft AD annuaire à l'aide d'Active Directory (AD) AWS Directory Service ou de votre annuaire autogéré dans Active Directory (AD), vous pouvez modifier la source d'identité de votre IAM Identity Center pour qu'elle fonctionne avec ces utilisateurs. Nous vous recommandons d'envisager de connecter cette source d'identité lorsque vous activez IAM Identity Center et que vous choisissez votre source d'identité. Cette opération avant de créer des utilisateurs et des groupes dans le répertoire par défaut d'Identity Center vous permettra d'éviter la configuration supplémentaire requise si vous modifiez votre source d'identité ultérieurement.

Pour utiliser Active Directory comme source d'identité, votre configuration doit répondre aux conditions préalables suivantes :

- Si vous utilisezAWS Managed Microsoft AD, vous devez activer IAM Identity Center au même Région AWS endroit où votre AWS Managed Microsoft AD annuaire est configuré. IAM Identity Center stocke les données d'attribution dans la même région que le répertoire. Pour administrer IAM Identity Center, vous devrez peut-être passer à la région dans laquelle IAM Identity Center est configuré. Notez également que le portail AWS d'accès utilise la même URL d'accès que votre annuaire.
- Utilisez un Active Directory résidant dans le compte de gestion :

  Vous devez disposer d'un AD Connector ou d'un AWS Managed Microsoft AD annuaire AD Connector existant dans votre compte de gestionAWS Directory Service, et celui-ci doit résider dans votre compte AWS Organizations de gestion. Vous ne pouvez connecter qu'un seul répertoire AD Connector ou un seul annuaire AWS Managed Microsoft AD à la fois. Si vous devez prendre en

charge plusieurs domaines ou forêts, utilisezAWS Managed Microsoft AD. Pour plus d'informations, consultez :

- Connecter un annuaire AWS Managed Microsoft AD à IAM Identity Center
- Connectez un annuaire autogéré dans Active Directory à IAM Identity Center

- Utilisez un Active Directory résidant dans le compte d'administrateur délégué :

  Si vous envisagez d'activer un administrateur délégué IAM Identity Center et d'utiliser Active Directory comme source d'identité IAM Identity Center, vous pouvez utiliser un AD Connector ou un AWS Managed Microsoft AD annuaire existant configuré dans AWS Directory résidant dans le compte d'administrateur délégué.

  Si vous décidez de remplacer la source d'identité IAM Identity Center d'une autre source par Active Directory, ou de la remplacer par une autre source, le répertoire doit résider dans le compte membre administrateur délégué d'IAM Identity Center (s'il en existe un) ; sinon, il doit se trouver dans le compte de gestion.

Ce didacticiel explique la configuration de base pour utiliser Active Directory comme source d'identité IAM Identity Center.

Étape 1 : Connecter Active Directory et spécifier un utilisateur

Si vous utilisez déjà Active Directory, les rubriques suivantes vous aideront à préparer la connexion de votre annuaire à IAM Identity Center.

> **Note**
>
> Pour des raisons de sécurité, nous vous recommandons vivement d'activer l'authentification multifactorielle. Si vous envisagez de connecter un AWS Managed Microsoft AD annuaire ou un annuaire autogéré dans Active Directory et que vous n'utilisez pas RADIUS MFA AWS Directory Service avec, activez l'authentification MFA dans IAM Identity Center.

AWS Managed Microsoft AD

1. Consultez les directives dansSe connecter à un Microsoft AD annuaire.
2. Suivez les étapes de Connecter un annuaire AWS Managed Microsoft AD à IAM Identity Center.

3. Configurez Active Directory pour synchroniser l'utilisateur auquel vous souhaitez accorder des autorisations administratives dans IAM Identity Center. Pour plus d'informations, consultez Synchroniser un utilisateur administratif dans IAM Identity Center.

Annuaire autogéré dans Active Directory

1. Consultez les directives dansSe connecter à un Microsoft AD annuaire.
2. Suivez les étapes de Connectez un annuaire autogéré dans Active Directory à IAM Identity Center.
3. Configurez Active Directory pour synchroniser l'utilisateur auquel vous souhaitez accorder des autorisations administratives dans IAM Identity Center. Pour plus d'informations, consultez Synchroniser un utilisateur administratif dans IAM Identity Center.

Étape 2 : Synchroniser un utilisateur administratif dans IAM Identity Center

Après avoir connecté votre annuaire à IAM Identity Center, vous pouvez spécifier un utilisateur auquel vous souhaitez accorder des autorisations administratives, puis synchroniser cet utilisateur depuis votre annuaire avec IAM Identity Center.

1. Ouvrez la console IAM Identity Center.
2. Sélectionnez Settings (Paramètres).
3. Sur la page Paramètres, choisissez l'onglet Source d'identité, sélectionnez Actions, puis sélectionnez Gérer la synchronisation.
4. Sur la page Gérer la synchronisation, choisissez l'onglet Utilisateurs, puis sélectionnez Ajouter des utilisateurs et des groupes.
5. Dans l'onglet Utilisateurs, sous Utilisateur, entrez le nom d'utilisateur exact et choisissez Ajouter.
6. Sous Utilisateurs et groupes ajoutés, procédez comme suit :
    a. Vérifiez que l'utilisateur auquel vous souhaitez accorder des autorisations administratives est spécifié.
    b. Cochez la case située à gauche du nom d'utilisateur.
    c. Sélectionnez Envoyer.
7. Sur la page Gérer la synchronisation, l'utilisateur que vous avez spécifié apparaît dans la liste Utilisateurs synchronisés.
8. Dans le panneau de navigation, choisissez utilisateurs.

9. Sur la page Utilisateurs, l'utilisateur que vous avez spécifié peut mettre un certain temps à apparaître dans la liste. Cliquez sur l'icône d'actualisation pour mettre à jour la liste des utilisateurs.

À ce stade, votre utilisateur n'a pas accès au compte de gestion. Vous allez configurer l'accès administratif à ce compte en créant un ensemble d'autorisations administratives et en affectant l'utilisateur à cet ensemble d'autorisations. Pour plus d'informations, consultez Crée un jeu d'autorisations..

Setting up SCIM provisioning between CyberArk and IAM Identity Center

IAM Identity Center prend en charge le provisionnement automatique (synchronisation) des informations utilisateur depuis CyberArk Directory Platform IAM Identity Center. Ce provisionnement utilise le protocole SCIM (System for Cross-Domain Identity Management) v2.0. Vous configurez cette connexion à CyberArk l'aide de votre point de terminaison SCIM et de votre jeton d'accès IAM Identity Center. Lorsque vous configurez la synchronisation SCIM, vous créez un mappage de vos attributs utilisateur avec CyberArk les attributs nommés dans IAM Identity Center. Cela entraîne la correspondance des attributs attendus entre IAM Identity Center etCyberArk.

Ce guide est basé sur CyberArk la version d'août 2021. Les étapes à suivre pour les nouvelles versions peuvent varier. Ce guide contient quelques remarques concernant la configuration de l'authentification utilisateur via SAML.

> **Note**
>
> Avant de commencer à déployer SCIM, nous vous recommandons de consulter d'abord leConsidérations relatives à l'utilisation du provisionnement automatique. Passez ensuite en revue les autres considérations dans la section suivante.

Rubriques

- (Facultatif) Étape 3 : Configuration des attributs utilisateur CyberArk pour le contrôle d'accès (ABAC) dans IAM Identity Center
- (Facultatif) Transmission d'attributs pour le contrôle d'accès

Prérequis

Vous aurez besoin des éléments suivants avant de pouvoir commencer :

- CyberArkabonnement ou essai gratuit. Pour vous inscrire à un essai gratuit, rendez-vous sur CyberArk.
- Un compte compatible avec IAM Identity Center (gratuit). Pour plus d'informations, voir Activer le centre d'identité IAM.
- Une connexion SAML entre votre CyberArk compte et IAM Identity Center, comme décrit dans la CyberArkdocumentation d'IAM Identity Center.
- Associez le connecteur IAM Identity Center aux rôles, utilisateurs et organisations auxquels vous souhaitez autoriser l'accès Comptes AWS.

Considérations relatives au SCIM

Voici les points à prendre en compte lors de l'utilisation CyberArk de la fédération pour IAM Identity Center :

- Seuls les rôles mappés dans la section Provisioning des applications seront synchronisés avec IAM Identity Center.
- Le script de provisionnement n'est pris en charge que dans son état par défaut. Une fois modifié, le provisionnement SCIM peut échouer.
  - Un seul attribut de numéro de téléphone peut être synchronisé et l'attribut par défaut est « téléphone professionnel ».
- Si le mappage des rôles dans l'application CyberArk IAM Identity Center est modifié, le comportement ci-dessous est attendu :
  - Si les noms de rôles sont modifiés, aucune modification n'est apportée aux noms de groupes dans IAM Identity Center.
  - Si les noms des groupes sont modifiés, de nouveaux groupes seront créés dans IAM Identity Center, les anciens groupes resteront mais n'auront aucun membre.

- Le comportement de synchronisation et de déprovisionnement des utilisateurs peut être configuré à partir de l'application CyberArk IAM Identity Center. Assurez-vous de configurer le comportement adapté à votre organisation. Voici les options qui s'offrent à vous :
  - Remplacez (ou non) les utilisateurs du répertoire Identity Center par le même nom principal.
  - Déprovisionnez les utilisateurs du centre d'identité IAM lorsque l'utilisateur est supprimé du CyberArk rôle.
  - Déprovisionner le comportement des utilisateurs : désactiver ou supprimer.

Étape 1 : activer le provisionnement dans IAM Identity Center

Dans cette première étape, vous utilisez la console IAM Identity Center pour activer le provisionnement automatique.

Pour activer le provisionnement automatique dans IAM Identity Center

1. Une fois que vous avez rempli les conditions requises, ouvrez la console IAM Identity Center.
2. Choisissez Paramètres dans le volet de navigation de gauche.
3. Sur la page Paramètres, recherchez la zone Informations de provisionnement automatique, puis choisissez Activer. Cela active immédiatement le provisionnement automatique dans IAM Identity Center et affiche les informations nécessaires sur le point de terminaison SCIM et le jeton d'accès.
4. Dans la boîte de dialogue de provisionnement automatique entrant, copiez chacune des valeurs des options suivantes. Vous devrez les coller ultérieurement lorsque vous configurerez le provisionnement dans votre IdP.
   a. Point de terminaison SCIM
   b. Jeton d'accès
5. Choisissez Fermer.

Maintenant que vous avez configuré le provisionnement dans la console IAM Identity Center, vous devez effectuer les tâches restantes à l'aide de l'application CyberArk IAM Identity Center. Ces étapes sont décrites dans la procédure suivante.

Étape 2 : configurer le provisionnement dans CyberArk

Utilisez la procédure suivante dans l'application CyberArk IAM Identity Center pour activer le provisionnement avec IAM Identity Center. Cette procédure suppose que vous avez déjà ajouté l'application CyberArk IAM Identity Center à votre console CyberArk d'administration sous Web Apps. Si vous ne l'avez pas encore fait, reportez-vous auPrérequis, puis suivez cette procédure pour configurer le provisionnement SCIM.

Pour configurer le provisionnement dans CyberArk

1. Ouvrez l'application CyberArk IAM Identity Center que vous avez ajoutée dans le cadre de la configuration de SAML pour CyberArk (Applications > Web App). veuillez consulter Prérequis.
2. Choisissez l'application IAM Identity Center et accédez à la section Provisioning.
3. Cochez la case Activer le provisionnement pour cette application et choisissez Live Mode.
4. Dans la procédure précédente, vous avez copié la valeur du point de terminaison SCIM depuis IAM Identity Center. Collez cette valeur dans le champ URL du service SCIM. Dans l'application CyberArk IAM Identity Center, définissez le type d'autorisation comme en-tête d'autorisation. Assurez-vous de supprimer la barre oblique à la fin de l'URL.
5. Définissez le type d'en-tête sur Bearer Token.
6. À partir de la procédure précédente, vous avez copié la valeur du jeton d'accès dans IAM Identity Center. Collez cette valeur dans le champ Bearer Token de l'application CyberArk IAM Identity Center.
7. Cliquez sur Vérifier pour tester et appliquer la configuration.
8. Dans les options de synchronisation, choisissez le comportement approprié pour lequel vous souhaitez que le provisionnement sortant fonctionneCyberArk. Vous pouvez choisir de remplacer (ou non) les utilisateurs IAM Identity Center existants par un nom principal et un comportement de déprovisionnement similaires.
9. Sous Mappage des rôles, configurez le mappage à partir CyberArk des rôles, dans le champ Nom, vers le groupe IAM Identity Center, sous le groupe de destination.
10. Cliquez sur Enregistrer en bas de page une fois que vous avez terminé.
11. Pour vérifier que les utilisateurs ont été correctement synchronisés avec IAM Identity Center, revenez à la console IAM Identity Center et sélectionnez Utilisateurs. Les utilisateurs synchronisés depuis CyberArk apparaîtront sur la page Utilisateurs. Ces utilisateurs peuvent désormais être affectés à des comptes et peuvent se connecter au sein d'IAM Identity Center.

(Facultatif) Étape 3 : Configuration des attributs utilisateur CyberArk pour le contrôle d'accès (ABAC) dans IAM Identity Center

Il s'agit d'une procédure facultative CyberArk si vous choisissez de configurer des attributs pour IAM Identity Center afin de gérer l'accès à vos AWS ressources. Les attributs que vous définissez CyberArk sont transmis dans une assertion SAML à IAM Identity Center. Vous créez ensuite un ensemble d'autorisations dans IAM Identity Center pour gérer l'accès en fonction des attributs que vous avez transmisCyberArk.

Avant de commencer cette procédure, vous devez d'abord activer la Attributs pour le contrôle d'accès fonctionnalité. Pour plus d'informations sur cette étape, consultez Activer et configurer les attributs pour le contrôle d'accès.

Pour configurer les attributs utilisateur CyberArk pour le contrôle d'accès dans IAM Identity Center

1. Ouvrez l'application CyberArk IAM Identity Center que vous avez installée dans le cadre de la configuration de SAML pour CyberArk (Apps > Web Apps).
2. Accédez à l'option SAML Response.
3. Sous Attributs, ajoutez les attributs appropriés au tableau en suivant la logique ci-dessous :
   a. Le nom de l'attribut est le nom d'attribut d'origine deCyberArk.
   b. La valeur d'attribut est le nom d'attribut envoyé dans l'assertion SAML à IAM Identity Center.
4. Choisissez Enregistrer.

(Facultatif) Transmission d'attributs pour le contrôle d'accès

Vous pouvez éventuellement utiliser la Attributs pour le contrôle d'accès fonctionnalité d'IAM Identity Center pour transmettre un `Attribute` élément dont l'`Name`attribut est défini sur. `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` Cet élément vous permet de transmettre des attributs en tant que balises de session dans l'assertion SAML. Pour plus d'informations sur les balises de session, consultez la section Transmission de balises de session AWS STSdans le guide de l'utilisateur IAM.

Pour transmettre des attributs en tant que balises de session, incluez l'élément `AttributeValue` qui spécifie la valeur de la balise. Par exemple, pour transmettre la paire clé-valeur du tag`CostCenter = blue`, utilisez l'attribut suivant.

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

Si vous devez ajouter plusieurs attributs, incluez un `Attribute` élément distinct pour chaque balise.

Configurer SAML et SCIM avec un IAM Google Workspace Identity Center

Si votre organisation l'utilise, Google Workspace vous pouvez intégrer vos utilisateurs et groupes depuis Google Workspace IAM Identity Center pour leur donner accès aux AWS ressources. Vous pouvez réaliser cette intégration en remplaçant la source d'identité par défaut de votre source d'identité IAM Identity Center par. Google Workspace

Les informations utilisateur provenant de Google Workspace sont synchronisées dans IAM Identity Center à l'aide du protocole System for Cross-Domain Identity Management (SCIM) v2.0. Vous configurez cette connexion en Google Workspace utilisant votre point de terminaison SCIM pour IAM Identity Center et un jeton porteur IAM Identity Center. Lorsque vous configurez la synchronisation SCIM, vous créez un mappage de vos attributs utilisateur avec Google Workspace les attributs nommés dans IAM Identity Center. Ce mappage correspond aux attributs utilisateur attendus entre IAM Identity Center etGoogle Workspace. Pour ce faire, vous devez vous configurer en Google Workspace tant que fournisseur d'identité IAM et fournisseur d'identité IAM Identity Center.

Objectif

Les étapes de ce didacticiel vous aident à établir la connexion SAML entre Google Workspace et AWS. Plus tard, vous synchroniserez les utilisateurs à Google Workspace l'aide de SCIM. Pour vérifier que tout est correctement configuré, une fois les étapes de configuration terminées, vous vous connecterez en tant qu'Google Workspaceutilisateur et vérifierez l'accès aux AWS ressources. Notez que ce didacticiel est basé sur un environnement de test de petits Google Workspace répertoires. Les structures de répertoire telles que les groupes et les unités organisationnelles ne sont pas incluses. Après avoir terminé ce didacticiel, vos utilisateurs pourront accéder au portail d' AWS accès avec vos Google Workspace informations d'identification.

> **Note**
>
> Pour vous inscrire à un essai gratuit ou Google Workspace rendez-vous Google Workspacesur le Google's site Web.
> Si vous n'avez pas encore activé IAM Identity Center, consultezActivant AWS IAM Identity Center.

Considérations

- Avant de configurer le provisionnement SCIM entre Google Workspace et IAM Identity Center, nous vous recommandons de vérifier. Considérations relatives à l'utilisation du provisionnement automatique
- La synchronisation automatique depuis SCIM Google Workspace est actuellement limitée au provisionnement des utilisateurs. Le provisionnement automatique des groupes n'est pas pris en charge pour le moment. Les groupes peuvent être créés manuellement à AWS CLI l'aide de la commande Identity Store create-group ou de l'API AWS Identity and Access Management (IAM). CreateGroup Vous pouvez également utiliser ssosync pour synchroniser Google Workspace les utilisateurs et les groupes dans IAM Identity Center.
- Chaque Google Workspace utilisateur doit avoir un prénom, un nom de famille, un nom d'utilisateur et une valeur de nom d'affichage spécifiés.
- Chaque Google Workspace utilisateur ne dispose que d'une seule valeur par attribut de données, tel qu'une adresse e-mail ou un numéro de téléphone. Les utilisateurs possédant plusieurs valeurs ne parviendront pas à se synchroniser. Si certains utilisateurs ont plusieurs valeurs dans leurs attributs, supprimez les attributs dupliqués avant de tenter de configurer l'utilisateur dans IAM Identity Center. Par exemple, un seul attribut de numéro de téléphone peut être synchronisé, étant donné que l'attribut de numéro de téléphone par défaut est « téléphone professionnel », utilisez l'attribut « téléphone professionnel » pour stocker le numéro de téléphone de l'utilisateur, même si le numéro de téléphone de l'utilisateur est un téléphone fixe ou un téléphone mobile.
- Les attributs sont toujours synchronisés si l'utilisateur est désactivé dans IAM Identity Center, mais toujours actif dans. Google Workspace
- Si un utilisateur existe déjà dans le répertoire Identity Center avec le même nom d'utilisateur et le même e-mail, il sera remplacé et synchronisé à l'aide de SCIM from. Google Workspace
- Des considérations supplémentaires doivent être prises en compte lors de la modification de votre source d'identité. Pour plus d'informations, consultez the section called "Passage d'IAM Identity Center à un IdP externe".

Étape 1 Google Workspace : Configuration de l'application SAML

1. Connectez-vous à votre console d'Googleadministration à l'aide d'un compte doté de privilèges de super administrateur.
2. Dans le panneau de navigation de gauche de votre console Google d'administration, sélectionnez Applications, puis Applications Web et mobiles.
3. Dans la liste déroulante Ajouter une application, sélectionnez Rechercher des applications.
4. Dans le champ de recherche, saisissez Amazon Web Services, puis sélectionnez l'application Amazon Web Services (SAML) dans la liste.
5. Sur la page Informations sur le fournisseur d'Googleidentité - Amazon Web Services, vous pouvez effectuer l'une des opérations suivantes :

   a. Téléchargez les métadonnées de l'IdP.

   b. Copiez l'URL SSO, l'URL de l'identifiant de l'entité et les informations du certificat.

   Vous aurez besoin du fichier XML ou des informations URL à l'étape 2.
6. Avant de passer à l'étape suivante dans la console Google d'administration, laissez cette page ouverte et passez à la console IAM Identity Center.

Étape 2 : IAM Identity Center et Google Workspace : Modification de la source d'identité IAM Identity Center et configuration en Google Workspace tant que fournisseur d'identité SAML

1. Connectez-vous à la console IAM Identity Center à l'aide d'un rôle doté d'autorisations administratives.
2. Choisissez Paramètres dans le volet de navigation de gauche.
3. Sur la page Paramètres, choisissez Actions, puis Modifier la source d'identité.

   - Si vous n'avez pas activé IAM Identity Center, consultez Activation du centre d'identité IAM pour plus d'informations. Après avoir activé et accédé à IAM Identity Center pour la première fois, vous arriverez au tableau de bord où vous pourrez sélectionner Choisissez votre source d'identité.
4. Sur la page Choisir une source d'identité, sélectionnez Fournisseur d'identité externe, puis cliquez sur Suivant.

5. La page Configurer le fournisseur d'identité externe s'ouvre. Pour compléter cette page et celle de l'Google Workspaceétape 1, vous devez effectuer les opérations suivantes :

   - Dans la section des métadonnées du fournisseur d'identité de la console IAM Identity Center, vous devez effectuer l'une des opérations suivantes :

     i. Téléchargez les métadonnées GoogleSAML en tant que métadonnées IDP SAML dans la console IAM Identity Center.

     ii. Copiez et collez l'URL GoogleSSO dans le champ URL de connexion IdP Google, l'URL de l'émetteur dans le champ URL de l'émetteur de l'IdP et téléchargez le certificat en tant que certificat IdP. Google

6. Après avoir fourni les Google métadonnées dans la section des métadonnées du fournisseur d'identité de la console IAM Identity Center, copiez l'URL de connexion au portail AWS d'accès, l'URL IAM Identity Assertion Consumer Service (ACS) et l'URL de l'émetteur du IAM Identity Center. Vous devrez fournir ces URL dans la console Google d'administration à l'étape suivante.
7. Laissez la page ouverte avec la console IAM Identity Center et revenez à la console Google d'administration. Vous devriez être sur la page de détails d'Amazon Web Services - Service Provider. Sélectionnez Continuer.
8. Sur la page de détails du fournisseur de services, entrez les valeurs de l'URL ACS, de l'ID d'entité et de l'URL de démarrage. Vous avez copié ces valeurs à l'étape précédente et elles se trouvent dans la console IAM Identity Center.

   - Collez l'URL du IAM Identity Center Assertion Consumer Service (ACS) dans le champ URL ACS
   - Collez l'URL de l'émetteur du IAM Identity Center dans le champ Entity ID.
   - Collez l'URL de connexion AWS au portail d'accès dans le champ URL de démarrage.

9. Sur la page de détails du fournisseur de services, complétez les champs sous le nom ID comme suit :

   - Pour le format Name ID, sélectionnez EMAIL
   - Pour Name ID, sélectionnez Informations de base **>** E-mail principal

10. Choisissez Continuer.
11. Sur la page Mappage d'attributs, sous Attributs, choisissez AJOUTER UN MAPPAGE, puis configurez les champs suivants sous Attribut de Google répertoire :

- Pour l'attribut de l'**`https://aws.amazon.com/SAML/Attributes/RoleSessionName`**application, sélectionnez le champ Informations de base, e-mail principal dans les Google Directoryattributs.
- Pour l'attribut de **`https://aws.amazon.com/SAML/Attributes/Role`** l'application, sélectionnez n'importe quel Google Directoryattribut. Un attribut de Google répertoire peut être Department.

12. Choisissez Finish
13. Revenez à la console IAM Identity Center et choisissez Next. Sur la page Vérifier et confirmer, passez en revue les informations, puis saisissez ACCEPT dans l'espace prévu à cet effet. Choisissez Modifier la source d'identité.

Vous êtes maintenant prêt à activer l'application Amazon Web Services Google Workspace afin que vos utilisateurs puissent être connectés à IAM Identity Center.

Étape 3 Google Workspace : Activez les applications

1. Retournez à la console Google d'administration et à votre AWS IAM Identity Center application, qui se trouvent sous Applications et applications Web et mobiles.
2. Dans le panneau Accès utilisateur situé à côté de Accès utilisateur, cliquez sur la flèche vers le bas pour étendre l'accès utilisateur afin d'afficher le panneau d'état du service.
3. Dans le panneau d'état du service, sélectionnez Activé pour tout le monde, puis sélectionnez ENREGISTRER.

> **Note**
>
> Pour respecter le principe du moindre privilège, nous vous recommandons de changer le statut du service sur OFF pour tous après avoir terminé ce didacticiel. Seuls les utilisateurs ayant besoin d'un accès AWS doivent avoir le service activé. Vous pouvez utiliser Google Workspace des groupes ou des unités organisationnelles pour donner aux utilisateurs l'accès à un sous-ensemble particulier de vos utilisateurs.

Étape 4 : IAM Identity Center : configurer le provisionnement automatique d'IAM Identity Center

1. Revenez à la console IAM Identity Center.
2. Sur la page Paramètres, recherchez la zone Informations de provisionnement automatique, puis choisissez Activer. Cela active immédiatement le provisionnement automatique dans IAM Identity Center et affiche les informations nécessaires sur le point de terminaison SCIM et le jeton d'accès.
3. Dans la boîte de dialogue de provisionnement automatique entrant, copiez chacune des valeurs des options suivantes. À l'étape 5 de ce didacticiel, vous allez entrer ces valeurs pour configurer le provisionnement automatique dansGoogle Workspace.

   - Point de terminaison SCIM
   - Jeton d'accès

   > **Warning**
   >
   > C'est le seul moment où vous pouvez obtenir le point de terminaison SCIM et le jeton d'accès. Assurez-vous de copier ces valeurs avant de continuer.

4. Choisissez Fermer.

   Maintenant que vous avez configuré le provisionnement dans la console IAM Identity Center, à l'étape suivante, vous allez configurer le provisionnement automatique dans. Google Workspace

Étape 5 Google Workspace : Configuration du provisionnement automatique

1. Retournez à la console Google d'administration et à votre AWS IAM Identity Center application, qui se trouvent sous Applications et applications Web et mobiles. Dans la section Approvisionnement automatique, choisissez Configurer le provisionnement automatique.
2. Dans la procédure précédente, vous avez copié la valeur du jeton d'accès dans la console IAM Identity Center. Collez cette valeur dans le champ du jeton d'accès et choisissez Continuer. Dans la procédure précédente, vous avez également copié la valeur du point de terminaison SCIM dans la console IAM Identity Center. Collez cette valeur dans le champ URL du point de terminaison. Assurez-vous de supprimer la barre oblique à la fin de l'URL et de sélectionner Continuer.

3. Vérifiez que tous les attributs obligatoires du centre d'identité IAM (ceux marqués d'un *) sont mappés aux Google Cloud Directory attributs. Dans le cas contraire, cliquez sur la flèche vers le bas et mappez vers l'attribut approprié. Choisissez Continuer.
4. Dans la section Provisioning Scope, vous pouvez choisir un groupe avec votre Google Workspace annuaire pour fournir un accès à l'application Amazon Web Services. Ignorez cette étape et sélectionnez Continuer.
5. Dans la section Déprovisionnement, vous pouvez choisir comment répondre aux différents événements qui suppriment l'accès à un utilisateur. Pour chaque situation, vous pouvez spécifier le délai avant le début du déprovisionnement afin de :

   - dans les 24 heures
   - après une journée
   - après sept jours
   - après 30 jours

   Chaque situation est assortie d'un délai pour suspendre l'accès à un compte et quand supprimer le compte.

   > **Tip**
   >
   > Prévoyez toujours plus de temps avant de supprimer le compte d'un utilisateur que pour le suspendre.

6. Choisissez Finish (Terminer). Vous êtes redirigé vers la page de l'application Amazon Web Services.
7. Dans la section Provisionnement automatique, activez le commutateur pour le faire passer d'Inactif à Actif.

   > **Note**
   >
   > Le curseur d'activation est désactivé si IAM Identity Center n'est pas activé pour les utilisateurs. Choisissez Accès utilisateur et activez l'application pour activer le curseur.

8. Dans la boîte de dialogue de confirmation, choisissez Activer.
9. Pour vérifier que les utilisateurs sont correctement synchronisés avec IAM Identity Center, revenez à la console IAM Identity Center et sélectionnez Utilisateurs. La page Utilisateurs

répertorie les utilisateurs de votre Google Workspace répertoire qui ont été créés par SCIM. Si les utilisateurs ne figurent pas encore dans la liste, il se peut que le provisionnement soit toujours en cours. Le provisionnement peut prendre jusqu'à 24 heures, mais dans la plupart des cas, il ne prend que quelques minutes. Assurez-vous d'actualiser la fenêtre du navigateur toutes les quelques minutes.

Sélectionnez un utilisateur et consultez ses informations. Les informations doivent correspondre à celles du Google Workspace répertoire.

Félicitations !

Vous avez correctement configuré une connexion SAML entre Google Workspace et AWS et vous avez vérifié que le provisionnement automatique fonctionne. Vous pouvez désormais attribuer ces utilisateurs à des comptes et à des applications dans IAM Identity Center. Pour ce didacticiel, à l'étape suivante, désignons l'un des utilisateurs comme administrateur du centre d'identité IAM en lui accordant des autorisations administratives sur le compte de gestion.

Étape 6 : IAM Identity Center : accorder aux Google Workspace utilisateurs l'accès aux comptes

1. Revenez à la console IAM Identity Center. Dans le volet de navigation d'IAM Identity Center, sous Autorisations multi-comptes, sélectionnez. Comptes AWS
2. Sur la Comptes AWSpage, la structure organisationnelle affiche la racine de votre organisation avec vos comptes en dessous dans la hiérarchie. Cochez la case correspondant à votre compte de gestion, puis sélectionnez Attribuer des utilisateurs ou des groupes.
3. Le flux de travail Attribuer des utilisateurs et des groupes s'affiche. Il comprend trois étapes :

    a. Pour l'étape 1 : Sélectionnez les utilisateurs et les groupes, choisissez l'utilisateur qui exécutera la fonction d'administrateur. Ensuite, sélectionnez Suivant.

    b. Pour l'étape 2 : Sélectionnez des ensembles d'autorisations, choisissez Créer un ensemble d'autorisations pour ouvrir un nouvel onglet qui vous indique les trois sous-étapes nécessaires à la création d'un ensemble d'autorisations.

        i. Pour l'étape 1 : Sélectionnez le type d'ensemble d'autorisations, procédez comme suit :

- Dans Type d'ensemble d'autorisations, choisissez Ensemble d'autorisations prédéfini.
- Dans Politique pour un ensemble d'autorisations prédéfini, sélectionnez AdministratorAccess.

Choisissez Suivant.

ii. Pour l'étape 2 : Spécifiez les détails de l'ensemble d'autorisations, conservez les paramètres par défaut et choisissez Next.

Les paramètres par défaut créent un ensemble d'autorisations nommé *AdministratorAccess*avec une durée de session fixée à une heure.

iii. Pour l'étape 3 : révision et création, vérifiez que le type d'ensemble d'autorisations utilise la politique AWS gérée AdministratorAccess. Choisissez Créer. Sur la page Ensembles d'autorisations, une notification apparaît pour vous informer que l'ensemble d'autorisations a été créé. Vous pouvez maintenant fermer cet onglet dans votre navigateur Web.

iv. Dans l'onglet du navigateur Attribuer des utilisateurs et des groupes, vous êtes toujours à l'étape 2 : sélectionnez les ensembles d'autorisations à partir desquels vous avez lancé le flux de travail de création d'ensembles d'autorisations.

v. Dans la zone Ensembles d'autorisations, cliquez sur le bouton Actualiser. L'ensemble *AdministratorAccess*d'autorisations que vous avez créé apparaît dans la liste. Cochez la case correspondant à cet ensemble d'autorisations, puis choisissez Next.

c. Pour l'étape 3 : vérifier et envoyer, passez en revue l'utilisateur et l'ensemble d'autorisations sélectionnés, puis choisissez Soumettre.

La page Compte AWS est mise à jour avec un message indiquant que vous êtes en cours de configuration. Attendez que le processus soit terminé.

Vous êtes renvoyé à la Comptes AWS page. Un message de notification vous informe que votre Compte AWS compte a été réapprovisionné et que l'ensemble d'autorisations mis à jour a été appliqué. Lorsque l'utilisateur se connecte, il a la possibilité de choisir le *AdministratorAccess*rôle.

> **Note**
>
> La synchronisation automatique SCIM depuis Google Workspace ne prend en charge que le provisionnement des utilisateurs. Le provisionnement automatique

des groupes n'est pas pris en charge pour le moment. Vous ne pouvez pas créer de groupes pour vos Google Workspace utilisateurs à l'aide du AWS Management Console. Après avoir configuré les utilisateurs, vous pouvez créer des groupes à l'aide de la commande AWS CLI Identity Store create-group ou de l'API IAM. CreateGroup

Étape 7 Google Workspace : Confirmer l'accès Google Workspace des utilisateurs aux AWS ressources

1. Connectez-vous à Google l'aide d'un compte utilisateur de test. Pour savoir comment ajouter des utilisateursGoogle Workspace, consultez Google Workspacela documentation.
2. Sélectionnez l'icône du Google apps lanceur (gaufre).
3. Faites défiler la liste des applications vers le bas où se trouvent vos Google Workspace applications personnalisées. Deux applications s'affichent : Amazon Web Services et le portail AWS d'accès.
4. Sélectionnez l'application du portail AWS d'accès. Vous êtes connecté au portail et vous pouvez voir l' Compte AWS icône. Développez cette icône pour voir la liste des Comptes AWS objets auxquels l'utilisateur peut accéder. Dans ce didacticiel, vous n'avez travaillé qu'avec un seul compte. Par conséquent, l'extension de l'icône ne permet d'afficher qu'un seul compte.

   > **Note**
   >
   > Si vous sélectionnez l'application Amazon Web Services, vous recevrez une erreur SAML. Cette application est utilisée pour Google Workspace les utilisateurs qui ont été configurés en tant qu'utilisateurs IAM et ce didacticiel fournit à vos utilisateurs le statut d'Google Workspaceutilisateurs dans IAM Identity Center.

5. Sélectionnez le compte pour afficher les ensembles d'autorisations disponibles pour l'utilisateur. Dans ce didacticiel, vous avez créé l'ensemble AdministratorAccessd'autorisations.
6. À côté de l'ensemble d'autorisations se trouvent des liens indiquant le type d'accès disponible pour cet ensemble d'autorisations. Lorsque vous avez créé l'ensemble d'autorisations, vous avez indiqué que la console de gestion et l'accès par programmation devaient être activés. Ces deux options sont donc présentes. Sélectionnez Console de gestion pour ouvrir le AWS Management Console.
7. L'utilisateur est connecté à la console.

(Facultatif) Transmission d'attributs pour le contrôle d'accès

Vous pouvez éventuellement utiliser la Attributs pour le contrôle d'accès fonctionnalité d'IAM Identity Center pour transmettre un `Attribute` élément dont l'`Name`attribut est défini sur. `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` Cet élément vous permet de transmettre des attributs en tant que balises de session dans l'assertion SAML. Pour plus d'informations sur les balises de session, consultez la section Transmission de balises de session AWS STS dans le guide de l'utilisateur IAM.

Pour transmettre des attributs en tant que balises de session, incluez l'élément `AttributeValue` qui spécifie la valeur de la balise. Par exemple, pour transmettre la paire clé-valeur du tag`CostCenter = blue`, utilisez l'attribut suivant.

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

Si vous devez ajouter plusieurs attributs, incluez un `Attribute` élément distinct pour chaque balise.

Étapes suivantes

Maintenant que vous avez configuré Google Workspace en tant que fournisseur d'identité et que vous avez configuré les utilisateurs dans IAM Identity Center, vous pouvez :

- Utilisez la commande AWS CLI Identity Store create-group ou l'API IAM CreateGrouppour créer des groupes pour vos utilisateurs.

  Les groupes sont utiles lors de l'attribution de l'accès aux applications Comptes AWS et de leur attribution. Plutôt que d'affecter chaque utilisateur individuellement, vous accordez des autorisations à un groupe. Plus tard, lorsque vous ajoutez ou supprimez des utilisateurs d'un groupe, l'utilisateur obtient ou perd l'accès dynamique aux comptes et aux applications que vous avez affectés au groupe.
- Configurez les autorisations en fonction des fonctions du travail, voir Création d'un ensemble d'autorisations.

  Les ensembles d'autorisations définissent le niveau d'accès des utilisateurs et des groupes à un Compte AWS. Les ensembles d'autorisations sont stockés dans IAM Identity Center et peuvent

être fournis à une ou plusieurs personnes. Comptes AWS Vous pouvez attribuer plus d'un jeu d'autorisations à un utilisateur.

> **Note**
>
> En tant qu'administrateur du centre d'identité IAM, vous devrez parfois remplacer les anciens certificats IdP par des certificats plus récents. Par exemple, vous devrez peut-être remplacer un certificat IdP lorsque la date d'expiration du certificat approche. Le processus de remplacement d'un ancien certificat par un nouveau est appelé rotation des certificats. Assurez-vous de vérifier comment gérer les certificats SAML pourGoogle Workspace.

Utilisation d'IAM Identity Center pour vous connecter à votre plateforme d'JumpCloudannuaire

IAM Identity Center prend en charge le provisionnement automatique (synchronisation) des informations utilisateur depuis JumpCloud Directory Platform vers IAM Identity Center. Ce provisionnement utilise le protocole SCIM (System for Cross-Domain Identity Management) v2.0. Vous configurez cette connexion à JumpCloud l'aide de votre point de terminaison SCIM et de votre jeton d'accès IAM Identity Center. Lorsque vous configurez la synchronisation SCIM, vous créez un mappage de vos attributs utilisateur avec JumpCloud les attributs nommés dans IAM Identity Center. Cela entraîne la correspondance des attributs attendus entre IAM Identity Center etJumpCloud.

Ce guide est basé sur JumpCloud la version de juin 2021. Les étapes à suivre pour les nouvelles versions peuvent varier. Ce guide contient quelques remarques concernant la configuration de l'authentification utilisateur via SAML.

Les étapes suivantes vous expliquent comment activer le provisionnement automatique des utilisateurs et des groupes depuis IAM Identity Center JumpCloud à l'aide du protocole SCIM.

> **Note**
>
> Avant de commencer à déployer SCIM, nous vous recommandons de consulter d'abord leConsidérations relatives à l'utilisation du provisionnement automatique. Passez ensuite en revue les autres considérations dans la section suivante.

Rubriques

Prérequis

Vous aurez besoin des éléments suivants avant de pouvoir commencer :

- JumpCloudabonnement ou essai gratuit. Pour vous inscrire à un essai gratuit, rendez-vous sur JumpCloud.
- Un compte compatible avec IAM Identity Center (gratuit). Pour plus d'informations, voir Activer le centre d'identité IAM.
- Une connexion SAML entre votre JumpCloud compte et IAM Identity Center, comme décrit dans la JumpClouddocumentation d'IAM Identity Center.
- Associez le connecteur IAM Identity Center aux groupes auxquels vous souhaitez autoriser l'accès aux AWS comptes.

Considérations relatives au SCIM

Les points suivants sont à prendre en compte lors de l'utilisation JumpCloud de la fédération pour IAM Identity Center.

- Seuls les groupes associés au connecteur AWS Single Sign-On JumpCloud seront synchronisés avec SCIM.
- Un seul attribut de numéro de téléphone peut être synchronisé et l'attribut par défaut est « téléphone professionnel ».
- Les noms et prénoms des utilisateurs de l'JumpCloudannuaire doivent être configurés pour être synchronisés avec IAM Identity Center avec SCIM.

- Les attributs sont toujours synchronisés si l'utilisateur est désactivé dans IAM Identity Center mais qu'il est toujours activé. JumpCloud
- Vous pouvez choisir d'activer la synchronisation SCIM uniquement pour les informations utilisateur en décochant la case « Activer la gestion des groupes d'utilisateurs et de l'appartenance aux groupes » dans le connecteur.
- Si un utilisateur existe déjà dans le répertoire Identity Center avec le même nom d'utilisateur et le même e-mail, il sera remplacé et synchronisé avec SCIM à partir de. JumpCloud

Étape 1 : activer le provisionnement dans IAM Identity Center

Dans cette première étape, vous utilisez la console IAM Identity Center pour activer le provisionnement automatique.

Pour activer le provisionnement automatique dans IAM Identity Center

1. Une fois que vous avez rempli les conditions requises, ouvrez la console IAM Identity Center.
2. Choisissez Paramètres dans le volet de navigation de gauche.
3. Sur la page Paramètres, recherchez la zone Informations de provisionnement automatique, puis choisissez Activer. Cela active immédiatement le provisionnement automatique dans IAM Identity Center et affiche les informations nécessaires sur le point de terminaison SCIM et le jeton d'accès.
4. Dans la boîte de dialogue de provisionnement automatique entrant, copiez chacune des valeurs des options suivantes. Vous devrez les coller ultérieurement lorsque vous configurerez le provisionnement dans votre IdP.
    a. Point de terminaison SCIM
    b. Jeton d'accès
5. Choisissez Fermer.

Maintenant que vous avez configuré le provisionnement dans la console IAM Identity Center, vous devez effectuer les tâches restantes à l'aide du connecteur JumpCloud IAM Identity Center. Ces étapes sont décrites dans la procédure suivante.

Étape 2 : configurer le provisionnement dans JumpCloud

Utilisez la procédure suivante dans le connecteur JumpCloud IAM Identity Center pour activer le provisionnement avec IAM Identity Center. Cette procédure suppose que vous avez déjà ajouté le connecteur JumpCloud IAM Identity Center à votre portail d'JumpCloudadministration et à vos groupes. Si vous ne l'avez pas encore fait, reportez-vous à cette procédurePrérequis, puis exécutez-la pour configurer le provisionnement SCIM.

Pour configurer le provisionnement dans JumpCloud

1. Ouvrez le connecteur JumpCloud IAM Identity Center que vous avez installé dans le cadre de la configuration de SAML pour JumpCloud (Authentification utilisateur > IAM Identity Center). veuillez consulter Prérequis.
2. Choisissez le connecteur IAM Identity Center, puis le troisième onglet Gestion des identités.
3. Cochez la case Activer la gestion des groupes d'utilisateurs et de l'appartenance aux groupes dans cette application si vous souhaitez que les groupes soient synchronisés avec SCIM.
4. Cliquez sur Configurer.
5. Dans la procédure précédente, vous avez copié la valeur du point de terminaison SCIM dans IAM Identity Center. Collez cette valeur dans le champ URL de base du connecteur JumpCloud IAM Identity Center. Assurez-vous de supprimer la barre oblique à la fin de l'URL.
6. À partir de la procédure précédente, vous avez copié la valeur du jeton d'accès dans IAM Identity Center. Collez cette valeur dans le champ Token Key du connecteur JumpCloud IAM Identity Center.
7. Cliquez sur Activer pour appliquer la configuration.
8. Assurez-vous d'avoir un indicateur vert à côté de l'authentification unique activée.
9. Passez au quatrième onglet Groupes d'utilisateurs et cochez les groupes que vous souhaitez approvisionner avec SCIM.
10. Cliquez sur Enregistrer en bas de page une fois que vous avez terminé.
11. Pour vérifier que les utilisateurs ont été correctement synchronisés avec IAM Identity Center, revenez à la console IAM Identity Center et sélectionnez Utilisateurs. Les utilisateurs synchronisés JumpCloud apparaissent sur la page Utilisateurs. Ces utilisateurs peuvent désormais être affectés à des comptes au sein d'IAM Identity Center.

(Facultatif) Étape 3 : Configuration des attributs utilisateur JumpCloud pour le contrôle d'accès dans IAM Identity Center

Il s'agit d'une procédure facultative JumpCloud si vous choisissez de configurer des attributs pour IAM Identity Center afin de gérer l'accès à vos AWS ressources. Les attributs que vous définissez JumpCloud sont transmis dans une assertion SAML à IAM Identity Center. Vous créez ensuite un ensemble d'autorisations dans IAM Identity Center pour gérer l'accès en fonction des attributs que vous avez transmisJumpCloud.

Avant de commencer cette procédure, vous devez d'abord activer la fonctionnalité Attributs pour le contrôle d'accès. Pour plus d'informations sur la procédure à suivre, voir Activer et configurer les attributs pour le contrôle d'accès.

Pour configurer les attributs utilisateur JumpCloud pour le contrôle d'accès dans IAM Identity Center

1. Ouvrez le connecteur JumpCloud IAM Identity Center que vous avez installé dans le cadre de la configuration de SAML pour JumpCloud (Authentification utilisateur > IAM Identity Center).
2. Choisissez le connecteur IAM Identity Center. Choisissez ensuite le deuxième onglet IAM Identity Center.
3. Au bas de cet onglet, vous trouverez le mappage des attributs utilisateur, choisissez Ajouter un nouvel attribut, puis procédez comme suit : vous devez effectuer ces étapes pour chaque attribut que vous allez ajouter afin de l'utiliser dans IAM Identity Center pour le contrôle d'accès.

    a. Dans le champ Nom de l'attribut du fournisseur de services, saisissez `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`AttributeName`**`.` Remplacer **`AttributeName`** par le nom de l'attribut que vous attendez dans IAM Identity Center. Par exemple, `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Email`**.

    b. Dans le champ Nom de JumpCloud l'attribut, sélectionnez les attributs utilisateur de votre JumpCloud répertoire. Par exemple, Email (Work).
4. Choisissez Enregistrer.

(Facultatif) Transmission d'attributs pour le contrôle d'accès

Vous pouvez éventuellement utiliser la Attributs pour le contrôle d'accès fonctionnalité d'IAM Identity Center pour transmettre un `Attribute` élément dont l'`Name`attribut est défini sur. `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`** Cet élément vous permet de transmettre des attributs en tant que balises de session dans l'assertion SAML. Pour plus

d'informations sur les balises de session, consultez la section Transmission de balises de session AWS STS dans le guide de l'utilisateur IAM.

Pour transmettre des attributs en tant que balises de session, incluez l'élément `AttributeValue` qui spécifie la valeur de la balise. Par exemple, pour transmettre la paire clé-valeur du tag`CostCenter = blue`, utilisez l'attribut suivant.

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

Si vous devez ajouter plusieurs attributs, incluez un `Attribute` élément distinct pour chaque balise.

Configurer SAML et SCIM avec un IAM Microsoft Entra ID Identity Center

AWS IAM Identity Centerprend en charge l'intégration avec le langage SAML (Security Assertion Markup Language) 2.0 ainsi que le provisionnement automatique (synchronisation) des informations sur les utilisateurs et les groupes Microsoft Entra ID (anciennement connu sous le nom de Azure Active Directory ouAzure AD) dans IAM Identity Center à l'aide du protocole System for Cross-domain Identity Management (SCIM) 2.0.

Objectif

Dans ce didacticiel, vous allez configurer un laboratoire de test et configurer une connexion SAML et un provisionnement SCIM entre IAM Identity Center Microsoft Entra ID et IAM. Au cours des étapes de préparation initiales, vous allez créer un utilisateur de test (Nikki Wolf) à la fois Microsoft Entra ID dans IAM Identity Center, que vous utiliserez pour tester la connexion SAML dans les deux sens. Plus tard, dans le cadre des étapes SCIM, vous créerez un autre utilisateur de test (Richard Roe) pour vérifier que les nouveaux attributs Microsoft Entra ID sont synchronisés avec IAM Identity Center comme prévu.

Prérequis

Avant de commencer ce didacticiel, vous devez d'abord configurer les éléments suivants :

- Un Microsoft Entra ID locataire. Pour plus d'informations, voir Démarrage rapide : configurer un client sur le site Web de Microsoft.
- Un compte AWS IAM Identity Center activé. Pour plus d'informations, consultez la section Activer le centre d'identité IAM dans le guide de l'AWS IAM Identity Centerutilisateur.

Étape 1 : préparer votre client Microsoft

Au cours de cette étape, vous allez découvrir comment installer et configurer votre application AWS IAM Identity Center d'entreprise et comment attribuer l'accès à un nouvel utilisateur de Microsoft Entra ID test.

Step 1.1 >

Étape 1.1 : Configuration de l'application AWS IAM Identity Center d'entreprise dans Microsoft Entra ID

Dans cette procédure, vous allez installer l'application AWS IAM Identity Center d'entreprise dansMicrosoft Entra ID. Vous aurez besoin de cette application ultérieurement pour configurer votre connexion SAML avecAWS.

1. Connectez-vous au centre d'administration Microsoft Entra en tant qu'administrateur d'applications cloud au moins.
2. Accédez à Identité > Applications > Applications d'entreprise, puis sélectionnez Nouvelle application.
3. Sur la page Parcourir la galerie Microsoft Entra, entrez **`AWS IAM Identity Center`**dans le champ de recherche.
4. Sélectionnez AWS IAM Identity Centerdans la zone de résultats.
5. Choisissez Créer.

Step 1.2 >

Étape 1.2 : créer un utilisateur de test dans Microsoft Entra ID

Nikki Wolf est le nom de l'utilisateur de Microsoft Entra ID test que vous allez créer dans cette procédure.

1. Dans la console du centre d'administration Microsoft Entra, accédez à Identité > Utilisateurs > Tous les utilisateurs.

2. Sélectionnez Nouvel utilisateur, puis choisissez Créer un nouvel utilisateur en haut de l'écran.
3. Dans Nom d'utilisateur principal, entrez **`NikkiWolf`**, puis sélectionnez le domaine et l'extension de votre choix. Par exemple, NikkiWolf@ *`exemple.org`*.
4. Dans Nom d'affichage, entrez **`NikkiWolf`**.
5. Dans Mot de passe, entrez un mot de passe fort ou sélectionnez l'icône en forme d'œil pour afficher le mot de passe généré automatiquement, puis copiez ou notez la valeur affichée.
6. Choisissez Propriétés, dans Prénom, entrez **`Nikki`**. Dans Nom de famille, entrez **`Wolf`**.
7. Choisissez Réviser + créer, puis sélectionnez Créer.

Step 1.3

Étape 1.3 : Testez l'expérience de Nikki avant d'attribuer ses autorisations à AWS IAM Identity Center

Au cours de cette procédure, vous allez vérifier ce que Nikki peut connecter avec succès à son portail Microsoft My Account.

1. Dans le même navigateur, ouvrez un nouvel onglet, accédez à la page de connexion au portail Mon compte et saisissez l'adresse e-mail complète de Nikki. Par exemple, NikkiWolf@ *`exemple.org`*.
2. Lorsque vous y êtes invité, entrez le mot de passe de Nikki, puis choisissez Se connecter. S'il s'agit d'un mot de passe généré automatiquement, vous serez invité à le modifier.
3. Sur la page Action requise, choisissez Demander plus tard pour ignorer l'invite à utiliser des méthodes de sécurité supplémentaires.
4. Sur la page Mon compte, dans le menu de navigation de gauche, sélectionnez Mes applications. Notez qu'à part les compléments, aucune application n'est affichée pour le moment. Vous allez ajouter une AWS IAM Identity Centerapplication qui apparaîtra ici lors d'une étape ultérieure.

Step 1.4

Étape 1.4 : Attribuer des autorisations à Nikki dans Microsoft Entra ID

Maintenant que vous avez vérifié que Nikki peut accéder au portail Mon compte, suivez cette procédure pour attribuer son utilisateur à l'AWS IAM Identity Centerapplication.

1. Dans la console du centre d'administration Microsoft Entra, accédez à Identité > Applications > Applications d'entreprise, puis AWS IAM Identity Centerchoisissez dans la liste.
2. Sur la gauche, sélectionnez Utilisateurs et groupes.
3. Choisissez Add user/group (Ajouter un utilisateur/groupe). Vous pouvez ignorer le message indiquant que les groupes ne sont pas disponibles pour l'attribution. Ce didacticiel n'utilise pas de groupes pour les devoirs.
4. Sur la page Ajouter une attribution, sous Utilisateurs, sélectionnez Aucune sélection.
5. Sélectionnez NikkiWolf, puis sélectionnez Sélectionner.
6. Sur la page Ajouter une affectation, choisissez Attribuer. NikkiWolf apparaît désormais dans la liste des utilisateurs assignés à l'AWS IAM Identity Centerapplication.

Étape 2 : Préparez votre AWS compte

Dans cette étape, vous découvrirez comment configurer les autorisations d'accès (via un ensemble d'autorisations), créer manuellement un utilisateur Nikki Wolf correspondant et lui attribuer les autorisations nécessaires pour administrer les ressources dansAWS. IAM Identity Center

Step 2.1 >

Étape 2.1 : Création d'un ensemble d' RegionalAdmin autorisations dans IAM Identity Center

Cet ensemble d'autorisations sera utilisé pour accorder à Nikki les autorisations de AWS compte nécessaires pour gérer les régions depuis la page Compte duAWS Management Console. Toutes les autres autorisations permettant de consulter ou de gérer d'autres informations relatives au compte de Nikki sont refusées par défaut.

1. Ouvrez la console IAM Identity Center.
2. Sous Autorisations multi-comptes, choisissez Ensembles d'autorisations.
3. Choisissez Create permission set (Créer un jeu d'autorisations).
4. Sur la page Sélectionner le type d'ensemble d'autorisations, sélectionnez Ensemble d'autorisations personnalisé, puis cliquez sur Suivant.
5. Sélectionnez Stratégie intégrée pour l'étendre, puis créez une politique pour l'ensemble d'autorisations en suivant les étapes suivantes :

    a. Choisissez Ajouter une nouvelle déclaration pour créer une déclaration de politique.

b. Sous Modifier le relevé, sélectionnez Compte dans la liste, puis cochez les cases suivantes.

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

c. À côté de Ajouter une ressource, choisissez Ajouter.

d. Sur la page Ajouter une ressource, sous Type de ressource, sélectionnez Toutes les ressources, puis choisissez Ajouter une ressource. Vérifiez que votre politique ressemble à ce qui suit :

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

6. Choisissez Suivant.
7. Sur la page Spécifier les détails de l'ensemble d'autorisations, sous Nom du jeu d'autorisations **`RegionalAdmin`**, entrez, puis choisissez Suivant.
8. Sur la page Review and create (Vérifier et créer), choisissez Create (Créer). Vous devriez RegionalAdminapparaître dans la liste des ensembles d'autorisations.

Step 2.2 >

Étape 2.2 : créer un NikkiWolf utilisateur correspondant dans IAM Identity Center

Étant donné que le protocole SAML ne fournit aucun mécanisme permettant d'interroger l'IdP Microsoft Entra ID () et de créer automatiquement des utilisateurs ici dans IAM Identity Center, utilisez la procédure suivante pour créer manuellement un utilisateur dans IAM Identity Center qui reflète les principaux attributs de l'utilisateur Nikki Wolfs dans. Microsoft Entra ID

1. Ouvrez la console IAM Identity Center.
2. Choisissez Utilisateurs, choisissez Ajouter un utilisateur, puis fournissez les informations suivantes :
   a. Pour le nom d'utilisateur et l'adresse e-mail : entrez le même **NikkiWolf@*yourcompanydomain.extension*** que celui que vous avez utilisé lors de la création de votre utilisateur. Microsoft Entra ID Par exemple, NikkiWolf@ *exemple.org*.
   b. Confirmer l'adresse e-mail — Entrez à nouveau l'adresse e-mail de l'étape précédente
   c. Prénom — Entrez **Nikki**
   d. Nom de famille — Entrez **Wolf**
   e. Nom d'affichage — Entrez **Nikki Wolf**
3. Choisissez Suivant deux fois, puis sélectionnez Ajouter un utilisateur.
4. Sélectionnez Fermer.

Step 2.3

Étape 2.3 : Attribuer Nikki aux RegionalAdmin autorisations définies dans IAM Identity Center

Vous trouvez ici les régions Compte AWS dans lesquelles Nikki administrera les régions, puis vous lui attribuez les autorisations nécessaires pour qu'elle puisse accéder correctement au portail AWS d'accès.

1. Ouvrez la console IAM Identity Center.
2. Sous Autorisations multi-comptes, choisissez Comptes AWS.
3. Cochez la case à côté du nom du compte (par exemple, *Sandbox) auquel* vous souhaitez accorder à Nikki l'accès pour gérer les régions, puis choisissez Attribuer des utilisateurs et des groupes.

4. Sur la page Attribuer des utilisateurs et des groupes, choisissez l'onglet Utilisateurs, recherchez et cochez la case à côté de Nikki, puis choisissez Suivant.

Étape 3 : configurer et tester votre connexion SAML

Au cours de cette étape, vous configurez votre connexion SAML à l'aide de l'application AWS IAM Identity Center d'entreprise Microsoft Entra ID ainsi que des paramètres IdP externes dans IAM Identity Center.

Step 3.1 >

Étape 3.1 : Collecter les métadonnées des fournisseurs de services requises auprès d'IAM Identity Center

Au cours de cette étape, vous lancerez l'assistant de modification de la source d'identité depuis la console IAM Identity Center et récupérerez le fichier de métadonnées et l'URL de connexion AWS spécifique que vous devrez saisir lors de la configuration de la connexion Microsoft Entra ID à l'étape suivante.

1. Dans la console IAM Identity Center, sélectionnez Paramètres.
2. Sur la page Paramètres, choisissez l'onglet Source d'identité, puis sélectionnez Actions > Modifier la source d'identité.
3. Sur la page Choisir une source d'identité, sélectionnez Fournisseur d'identité externe, puis cliquez sur Suivant.
4. Sur la page Configurer le fournisseur d'identité externe, sous Métadonnées du fournisseur de services, choisissez Télécharger le fichier de métadonnées pour le télécharger sur votre système.
5. Dans la même section, recherchez la valeur de l'URL de connexion AWS au portail d'accès et copiez-la. Vous devrez saisir cette valeur lorsque vous y serez invité à l'étape suivante.
6. Laissez cette page ouverte et passez à l'étape suivante (**`Step 3.2`**) pour configurer l'application AWS IAM Identity Center d'entreprise dansMicrosoft Entra ID. Plus tard, vous reviendrez sur cette page pour terminer le processus.

Step 3.2 >

Étape 3.2 : Configuration de l'application AWS IAM Identity Center d'entreprise dans Microsoft Entra ID

Cette procédure établit la moitié de la connexion SAML côté Microsoft en utilisant les valeurs du fichier de métadonnées et de l'URL de connexion que vous avez obtenues à l'étape précédente.

1. Dans la console du centre d'administration Microsoft Entra, accédez à Identité > Applications > Applications d'entreprise, puis choisissez AWS IAM Identity Center.
2. Sur la gauche, sélectionnez Authentification unique.
3. Sur la page Configurer l'authentification unique avec SAML, choisissez Télécharger le fichier de métadonnées, choisissez l'icône du dossier, sélectionnez le fichier de métadonnées du fournisseur de services que vous avez téléchargé à l'étape précédente, puis choisissez Ajouter.
4. Sur la page de configuration SAML de base, vérifiez que les valeurs de l'identifiant et de l'URL de réponse AWS pointent désormais vers des points de terminaison commençant par. `https://<REGION>.signin.aws.amazon.com/platform/saml/`
5. Sous URL de connexion (facultatif), collez la valeur de l'URL de connexion AWS au portail d'accès que vous avez copiée à l'étape précédente (**`Step 3.1`**), choisissez Enregistrer, puis X pour fermer la fenêtre.
6. Si vous êtes invité à tester l'authentification unique avecAWS IAM Identity Center, choisissez Non, je testerai plus tard. Vous effectuerez cette vérification dans une étape ultérieure.
7. Sur la page Configurer l'authentification unique avec SAML, dans la section Certificats SAML, à côté de Federation Metadata XML, choisissez Télécharger pour enregistrer le fichier de métadonnées sur votre système. Vous devrez télécharger ce fichier lorsque vous y serez invité à l'étape suivante.

Step 3.3 >

Étape 3.3 : Configuration de l'IdP Microsoft Entra ID externe dans AWS IAM Identity Center

Ici, vous allez revenir à l'assistant de modification de la source d'identité de la console IAM Identity Center pour terminer la seconde moitié de la connexion SAML. AWS

1. Revenez à la session de navigateur que vous avez laissée ouverte **`Step 3.1`**dans la console IAM Identity Center.
2. Sur la page Configurer le fournisseur d'identité externe, dans la section Métadonnées du fournisseur d'identité, sous Métadonnées IDP SAML, cliquez sur le bouton Choisir un fichier,

sélectionnez le fichier de métadonnées du fournisseur d'identité à partir duquel vous avez téléchargé Microsoft Entra ID à l'étape précédente, puis choisissez Ouvrir.

3. Choisissez Suivant.
4. Après avoir lu la clause de non-responsabilité et être prêt à continuer, entrez **ACCEPT**.
5. Choisissez Modifier la source d'identité pour appliquer vos modifications.

Step 3.4 >

Étape 3.4 : Vérifiez que Nikki est redirigée vers le portail AWS d'accès

Dans cette procédure, vous allez tester la connexion SAML en vous connectant au portail My Account de Microsoft avec les informations d'identification de Nikki. Une fois authentifié, vous allez sélectionner l'AWS IAM Identity Centerapplication qui redirigera Nikki vers le portail d'AWSaccès.

1. Accédez à la page de connexion au portail Mon compte et saisissez l'adresse e-mail complète de Nikki. Par exemple, ***NikkiWolf***@ *exemple.org*.
2. Lorsque vous y êtes invité, entrez le mot de passe de Nikki, puis choisissez Se connecter.
3. Sur la page Mon compte, dans le menu de navigation de gauche, sélectionnez Mes applications.
4. Sur la page Mes applications, sélectionnez l'application nommée AWS IAM Identity Center. Cela devrait vous demander une authentification supplémentaire.
5. Sur la page de connexion de Microsoft, choisissez vos NikkiWolf informations d'identification. Si vous êtes invité une deuxième fois à vous authentifier, sélectionnez à nouveau vos NikkiWolf informations d'identification. Cela devrait vous rediriger automatiquement vers le portail AWS d'accès.

> **Tip**
>
> Si vous n'êtes pas redirigé correctement, assurez-vous que la valeur de l'URL de connexion AWS au portail d'accès que vous avez saisie **Step 3.2**correspond à la valeur que vous avez copiée **Step 3.1**.

6. Vérifiez qu'une icône de AWScompte

s'affiche.

> **Tip**
>
> Si la page est vide et qu'aucune icône de AWScompte n'est affichée, vérifiez que Nikki a bien été affectée à l'ensemble RegionalAdmind'autorisations (voir **`Step 2.3`**).

Step 3.5

Étape 3.5 : Testez le niveau d'accès de Nikki pour la gérer Compte AWS

Au cours de cette étape, vous allez vérifier le niveau d'accès de Nikki pour gérer les paramètres régionaux pour elleCompte AWS. Nikki ne doit disposer de privilèges d'administrateur suffisants que pour gérer les régions depuis la page des comptes.

1. Dans le portail AWS d'accès, cliquez sur l'icône AWSCompte

   pour développer la liste des comptes. Après avoir choisi l'icône, les noms de compte, les identifiants de compte et les adresses e-mail associés à tous les comptes pour lesquels vous avez défini des ensembles d'autorisations apparaissent.
2. Choisissez le nom du compte (par exemple, *`Sandbox`*) sur lequel vous avez appliqué l'ensemble d'autorisations (voir **`Step 2.3`**). Cela élargira la liste des ensembles d'autorisations parmi lesquels Nikki pourra choisir pour gérer son compte.
3. Ensuite, RegionalAdminchoisissez la console de gestion pour assumer le rôle que vous avez défini dans le jeu RegionalAdmind'autorisations. Cela vous redirigera vers la page d'AWS Management Consoleaccueil.
4. Dans le coin supérieur droit de la console, choisissez le nom de votre compte, puis sélectionnez Compte. Vous serez redirigé vers la page du compte. Notez que toutes les autres sections de cette page affichent un message indiquant que vous ne disposez pas des autorisations nécessaires pour afficher ou modifier ces paramètres.
5. Sur la page Compte, faites défiler la page vers le bas jusqu'à la section AWSRégions. Cochez une case pour n'importe quelle région disponible dans le tableau. Notez que Nikki dispose des autorisations nécessaires pour activer ou désactiver la liste des régions pour son compte, comme prévu.

> **Bien fait !**
>
> Les étapes 1 à 3 vous ont aidé à implémenter et à tester avec succès votre connexion SAML. Maintenant, pour terminer le didacticiel, nous vous encourageons à passer à l'étape 4 pour implémenter le provisionnement automatique.

Étape 4 : configurer et tester votre synchronisation SCIM

Au cours de cette étape, vous allez configurer le provisionnement automatique (synchronisation) des informations utilisateur depuis Microsoft Entra ID IAM Identity Center à l'aide du protocole SCIM v2.0. Vous configurez cette connexion en Microsoft Entra ID utilisant votre point de terminaison SCIM pour IAM Identity Center et un jeton porteur créé automatiquement par IAM Identity Center.

Lorsque vous configurez la synchronisation SCIM, vous créez un mappage de vos attributs utilisateur avec Microsoft Entra ID les attributs nommés dans IAM Identity Center. Cela entraîne la correspondance des attributs attendus entre IAM Identity Center etMicrosoft Entra ID.

Les étapes suivantes vous expliquent comment activer le provisionnement automatique des utilisateurs résidant principalement dans IAM Identity Center Microsoft Entra ID à l'aide de l'application IAM Identity Center dans. Microsoft Entra ID

Step 4.1 >

Étape 4.1 : créer un deuxième utilisateur de test dans Microsoft Entra ID

À des fins de test, vous allez créer un nouvel utilisateur (Richard Roe) dansMicrosoft Entra ID. Plus tard, après avoir configuré la synchronisation SCIM, vous testerez que cet utilisateur et tous les attributs pertinents ont été correctement synchronisés avec IAM Identity Center.

1. Dans la console du centre d'administration Microsoft Entra, accédez à Identité > Utilisateurs > Tous les utilisateurs.
2. Sélectionnez Nouvel utilisateur, puis choisissez Créer un nouvel utilisateur en haut de l'écran.
3. Dans Nom d'utilisateur principal, entrez **`RichRoe`**, puis sélectionnez le domaine et l'extension de votre choix. Par exemple, RichRoe@ *`exemple.org`*.
4. Dans Nom d'affichage, entrez **`RichRoe`**.
5. Dans Mot de passe, entrez un mot de passe fort ou sélectionnez l'icône en forme d'œil pour afficher le mot de passe généré automatiquement, puis copiez ou notez la valeur affichée.

6. Choisissez Propriétés, puis indiquez les valeurs suivantes :
   - Prénom - Entrez **`Richard`**
   - Nom de famille - Enter **`Roe`**
   - Intitulé du poste - Entrez **`Marketing Lead`**
   - Département - Entrez **`Sales`**
   - ID d'employé - Entrez **`12345`**
7. Choisissez Réviser + créer, puis sélectionnez Créer.

Step 4.2 >

Étape 4.2 : activer le provisionnement automatique dans IAM Identity Center

Dans cette procédure, vous allez utiliser la console IAM Identity Center pour activer le provisionnement automatique des utilisateurs et des groupes provenant d'IAM Microsoft Entra ID Identity Center.

1. Ouvrez la console IAM Identity Center, puis sélectionnez Paramètres dans le volet de navigation de gauche.
2. Sur la page Paramètres, sous l'onglet Source d'identité, notez que la méthode de provisionnement est définie sur Manuel.
3. Localisez la zone Informations de provisionnement automatique, puis choisissez Activer. Cela active immédiatement le provisionnement automatique dans IAM Identity Center et affiche les informations nécessaires sur le point de terminaison SCIM et le jeton d'accès.
4. Dans la boîte de dialogue de provisionnement automatique entrant, copiez chacune des valeurs des options suivantes. Vous devrez les coller à l'étape suivante lorsque vous configurerez le provisionnement dansMicrosoft Entra ID.
   a. Point de terminaison SCIM : par exemple, https://scim. *`us-east-2 .amazonaws.com/ 111111111-2222-3333-4444-55555555555555 /scim/v2/`*
   b. Jeton d'accès : choisissez Afficher le jeton pour copier la valeur.
5. Choisissez Fermer.
6. Dans l'onglet Source d'identité, notez que la méthode de provisionnement est désormais définie sur SCIM.

Step 4.3 >

Étape 4.3 : Configuration du provisionnement automatique dans Microsoft Entra ID

Maintenant que votre utilisateur de RichRoe test est en place et que vous avez activé le SCIM dans IAM Identity Center, vous pouvez procéder à la configuration des paramètres de synchronisation SCIM dans. Microsoft Entra ID

1. Dans la console du centre d'administration Microsoft Entra, accédez à Identité > Applications > Applications d'entreprise, puis choisissez AWS IAM Identity Center.
2. Choisissez Provisioning, sous Manage, choisissez à nouveau Provisioning.
3. En mode de provisionnement, sélectionnez Automatique.
4. Sous Informations d'identification de l'administrateur, dans URL du locataire, collez la valeur de l'URL du point de terminaison SCIM que vous avez copiée **`Step 4.1`**précédemment. Dans Secret Token, collez la valeur du jeton d'accès.
5. Choisissez Test Connection (Connexion test). Vous devriez voir un message indiquant que les informations d'identification testées ont été correctement autorisées pour activer le provisionnement.
6. Choisissez Enregistrer.
7. Sous Gérer, sélectionnez Utilisateurs et groupes, puis choisissez Ajouter un utilisateur/un groupe.
8. Sur la page Ajouter une attribution, sous Utilisateurs, sélectionnez Aucune sélection.
9. Sélectionnez RichRoe, puis sélectionnez Sélectionner.
10. Sur la page Add Assignment (Ajouter une affectation), sélectionnez Assign (Affecter).
11. Choisissez Vue d'ensemble, puis sélectionnez Démarrer le provisionnement.

Step 4.4

Étape 4.4 : vérifier que la synchronisation a bien eu lieu

Dans cette section, vous allez vérifier que l'utilisateur de Richard a été correctement configuré et que tous les attributs sont affichés dans IAM Identity Center.

1. Dans la console IAM Identity Center, sélectionnez Users.
2. Sur la page Utilisateurs, vous devriez voir votre nom RichRoed'utilisateur affiché. Notez que dans la colonne Created by, la valeur est définie sur SCIM.

3. Choisissez RichRoe, sous Profil, de vérifier que les attributs suivants ont été copiés à partir deMicrosoft Entra ID.

   - Prénom - **`Richard`**
   - Nom de famille - **`Roe`**
   - Département - **`Sales`**
   - Titre - **`Marketing Lead`**
   - Numéro d'employé - **`12345`**

   Maintenant que l'utilisateur de Richard a été créé dans IAM Identity Center, vous pouvez l'attribuer à n'importe quel ensemble d'autorisations afin de contrôler le niveau d'accès dont il dispose à vos AWS ressources. Par exemple, vous pouvez attribuer RichRoeà l'ensemble d'**`RegionalAdmin`**autorisations que vous avez utilisé précédemment pour accorder à Nikki les autorisations nécessaires pour gérer les régions (voir **`Step 2.3`**), puis tester son niveau d'accès à l'aide **`Step 3.5`**de.

> **Félicitations !**
>
> Vous avez correctement configuré une connexion SAML entre Microsoft AWS et vous avez vérifié que le provisionnement automatique fonctionne pour que tout reste synchronisé. Vous pouvez désormais appliquer ce que vous avez appris pour configurer plus facilement votre environnement de production.

Considérations relatives à l'utilisation de SCIM Microsoft Entra ID dans un environnement de production

Voici quelques considérations importantes Microsoft Entra ID qui peuvent affecter la manière dont vous prévoyez de mettre en œuvre le provisionnement automatique avec IAM Identity Center dans votre environnement de production à l'aide du protocole SCIM v2.

> **Note**
>
> Avant de commencer à déployer le SCIM, nous vous recommandons de procéder à un premier examenConsidérations relatives à l'utilisation du provisionnement automatique.

Attributs pour le contrôle d'accès

Les attributs de contrôle d'accès sont utilisés dans les politiques d'autorisation qui déterminent qui, dans votre source d'identité, peut accéder à vos AWS ressources. Si un attribut est supprimé d'un utilisateur dansMicrosoft Entra ID, cet attribut ne sera pas supprimé de l'utilisateur correspondant dans IAM Identity Center. Il s'agit d'une limitation connue dansMicrosoft Entra ID. Si un attribut est remplacé par une valeur différente (non vide) pour un utilisateur, cette modification sera synchronisée avec IAM Identity Center.

Groupes imbriqués

Le service de provisionnement des Microsoft Entra ID utilisateurs ne peut ni lire ni approvisionner les utilisateurs dans des groupes imbriqués. Seuls les utilisateurs qui sont membres immédiats d'un groupe explicitement assigné peuvent être lus et approvisionnés. Microsoft Entra IDne décompresse pas de manière récursive les appartenances aux groupes ou utilisateurs assignés indirectement (utilisateurs ou groupes membres d'un groupe directement attribué). Pour plus d'informations, consultez la section Délimitation basée sur les assignations dans la documentation. Microsoft Entra ID

Groupes dynamiques

Le service de provisionnement des Microsoft Entra ID utilisateurs peut lire et provisionner les utilisateurs dans des groupes dynamiques. Vous trouverez ci-dessous un exemple illustrant la structure des utilisateurs et des groupes lors de l'utilisation de groupes dynamiques et la manière dont ils sont affichés dans IAM Identity Center. Ces utilisateurs et groupes ont été approvisionnés depuis Microsoft Entra ID IAM Identity Center via SCIM

Par exemple, si Microsoft Entra ID la structure des groupes dynamiques est la suivante :

1. Groupe A avec les membres ua1, ua2
2. Groupe B avec membres ub1
3. Groupe C avec membres uc1
4. Groupe K avec une règle pour inclure les membres des groupes A, B, C
5. Groupe L avec une règle pour inclure les membres des groupes B et C

Une fois que les informations sur les utilisateurs et les groupes ont été Microsoft Entra ID fournies depuis IAM Identity Center via SCIM, la structure sera la suivante :

1. Groupe A avec les membres ua1, ua2

2. Groupe B avec membres ub1
3. Groupe C avec membres uc1
4. Groupe K avec les membres ua1, ua2, ub1, uc1
5. Groupe L avec membres ub1, uc1

Lorsque vous configurez le provisionnement automatique à l'aide de groupes dynamiques, tenez compte des considérations suivantes.

- Un groupe dynamique peut inclure un groupe imbriqué. Cependant, le service de Microsoft Entra ID provisionnement n'aplatit pas le groupe imbriqué. Par exemple, si vous avez la Microsoft Entra ID structure suivante pour les groupes dynamiques :
  - Le groupe A est le parent du groupe B.
  - Le groupe A compte ua1 comme membre.
  - Le groupe B a ub1 comme membre.

Le groupe dynamique qui inclut le groupe A inclura uniquement les membres directs du groupe A (c'est-à-dire ua1). Il n'inclura pas de manière récursive les membres du groupe B.

- Les groupes dynamiques ne peuvent pas contenir d'autres groupes dynamiques. Pour plus d'informations, consultez la section Limitations relatives à la prévisualisation dans la Microsoft Entra ID documentation.

Résolution des problèmes liés au SCIM avec Microsoft Entra ID

Si vous rencontrez des problèmes lorsque Microsoft Entra ID les utilisateurs ne se synchronisent pas avec IAM Identity Center, cela peut être dû à un problème de syntaxe signalé par IAM Identity Center lorsqu'un nouvel utilisateur est ajouté à IAM Identity Center. Vous pouvez le confirmer en vérifiant les journaux Microsoft Entra ID d'audit pour détecter les événements ayant échoué, tels qu'un `'Export'`. Le motif du statut de cet événement indiquera :

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

Vous pouvez également vérifier AWS CloudTrail l'échec de l'événement. Cela peut être fait en effectuant une recherche dans la console de l'historique des événements CloudTrail ou en utilisant le filtre suivant :

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

L'erreur de l' CloudTrail événement indiquera ce qui suit :

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

En fin de compte, cette exception signifie que l'une des valeurs transmises Microsoft Entra ID contenait plus de valeurs que prévu. La solution consiste à examiner les attributs de l'utilisateur dansMicrosoft Entra ID, en veillant à ce qu'aucun ne contienne de valeurs dupliquées. Un exemple courant de valeurs dupliquées est la présence de plusieurs valeurs pour les numéros de contact tels que les numéros de téléphone portable, professionnel et de télécopie. Bien que les valeurs soient distinctes, elles sont toutes transmises à IAM Identity Center sous l'attribut parent unique PhoneNumbers.

Pour obtenir des conseils généraux de résolution des problèmes liés au SCIM, consultezRésolution des problèmes liés à IAM Identity Center.

Étape 5 : (Facultatif) Configurer ABAC

Maintenant que vous avez correctement configuré SAML et SCIM, vous pouvez éventuellement choisir de configurer le contrôle d'accès basé sur les attributs (ABAC). L'ABAC est une stratégie d'autorisation qui définit les autorisations en fonction des attributs.

AvecMicrosoft Entra ID, vous pouvez utiliser l'une des deux méthodes suivantes pour configurer ABAC afin de l'utiliser avec IAM Identity Center.

Method 1

> Méthode 1 : Configuration des attributs utilisateur Microsoft Entra ID pour le contrôle d'accès dans IAM Identity Center
>
> Dans la procédure suivante, vous allez déterminer quels attributs Microsoft Entra ID doivent être utilisés par IAM Identity Center pour gérer l'accès à vos AWS ressources. Une fois définis, Microsoft Entra ID envoie ces attributs à IAM Identity Center via des assertions SAML. Vous devrez ensuite accéder Crée un jeu d'autorisations. à IAM Identity Center pour gérer l'accès en fonction des attributs que vous avez transmisMicrosoft Entra ID.

Avant de commencer cette procédure, vous devez d'abord activer la Attributs pour le contrôle d'accès fonctionnalité. Pour plus d'informations sur cette étape, consultez Activer et configurer les attributs pour le contrôle d'accès.

1. Dans la console du centre d'administration Microsoft Entra, accédez à Identité > Applications > Applications d'entreprise, puis choisissez AWS IAM Identity Center.
2. Choisissez Single sign-on (Authentification unique).
3. Dans la section Attributs et revendications, choisissez Modifier.
4. Sur la page Attributs et réclamations, procédez comme suit :
   a. Choisissez Ajouter une nouvelle réclamation
   b. Pour Name (Nom), saisissez `AccessControl:`*`AttributeName`*. *`AttributeName`*Remplacez-le par le nom de l'attribut que vous attendez dans IAM Identity Center. Par exemple, `AccessControl:`**`Department`**.
   c. Pour Espace de noms, saisissez **`https://aws.amazon.com/SAML/Attributes`**.
   d. Pour Source, choisissez Attribut.
   e. Pour Attribut source, utilisez la liste déroulante pour sélectionner les attributs Microsoft Entra ID utilisateur. Par exemple, `user.`**`department`**.
5. Répétez l'étape précédente pour chaque attribut que vous devez envoyer à IAM Identity Center dans l'assertion SAML.
6. Choisissez Enregistrer.

Method 2

Méthode 2 : configurer ABAC à l'aide d'IAM Identity Center

Avec cette méthode, vous utilisez la Attributs pour le contrôle d'accès fonctionnalité d'IAM Identity Center pour transmettre un `Attribute` élément dont l'`Name`attribut est défini sur. `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`** Vous pouvez utiliser cet élément pour transmettre des attributs sous forme de balises de session dans l'assertion SAML. Pour plus d'informations sur les balises de session, consultez la section Transmission de balises de session AWS STS dans le guide de l'utilisateur IAM.

Pour transmettre des attributs en tant que balises de session, incluez l'élément `AttributeValue` qui spécifie la valeur de la balise. Par exemple, pour transmettre la paire clé-valeur du tag`CostCenter = blue`, utilisez l'attribut suivant :

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

Si vous devez ajouter plusieurs attributs, incluez un `Attribute` élément distinct pour chaque balise.

Configurer SAML et SCIM avec un IAM Okta Identity Center

Vous pouvez automatiquement approvisionner (synchroniser) les informations des utilisateurs et des groupes depuis Okta IAM Identity Center à l'aide du protocole SCIM (System for Cross-Domain Identity Management) v2.0. Pour configurer cette connexionOkta, vous utilisez votre point de terminaison SCIM pour IAM Identity Center et un jeton porteur créé automatiquement par IAM Identity Center. Lorsque vous configurez la synchronisation SCIM, vous créez un mappage de vos attributs utilisateur avec Okta les attributs nommés dans IAM Identity Center. Ce mappage correspond aux attributs utilisateur attendus entre IAM Identity Center et votreOkta.

Oktaprend en charge les fonctionnalités de provisionnement suivantes lorsqu'il est connecté à IAM Identity Center via SCIM :

- Créer des utilisateurs : les utilisateurs affectés à l'application IAM Identity Center dans Okta sont provisionnés dans IAM Identity Center.
- Mettre à jour les attributs utilisateur : les modifications d'attributs pour les utilisateurs affectés à l'application IAM Identity Center Okta sont mises à jour dans IAM Identity Center.
- Désactiver les utilisateurs : les utilisateurs qui ne sont pas affectés par l'application IAM Identity Center dans Okta sont désactivés dans IAM Identity Center.
- Push de groupe : les groupes (et leurs membres) Okta sont synchronisés avec IAM Identity Center.

> **Note**
>
> Pour minimiser les frais administratifs, tant Okta pour IAM Identity Center, que pour IAM Identity Center, nous vous recommandons d'attribuer et de transférer des groupes plutôt que des utilisateurs individuels.

Si vous n'avez pas encore activé IAM Identity Center, consultezActivant AWS IAM Identity Center.

Objectif

Dans ce didacticiel, vous allez découvrir comment configurer une connexion SAML avec Okta IAM Identity Center. Plus tard, vous synchroniserez les utilisateurs depuisOkta, à l'aide de SCIM. Dans ce scénario, vous gérez tous les utilisateurs et groupes dansOkta. Les utilisateurs se connectent via le Okta portail. Pour vérifier que tout est correctement configuré, une fois les étapes de configuration terminées, vous vous connecterez en tant qu'Oktautilisateur et vérifierez l'accès aux AWS ressources.

> **Note**
>
> Vous pouvez créer un Okta compte (essai gratuit) sur lequel l'application Okta's IAM Identity Center est installée. Pour les Okta produits payants, vous devrez peut-être confirmer que votre Okta licence prend en charge la gestion du cycle de vie ou des fonctionnalités similaires permettant le provisionnement sortant. Ces fonctionnalités peuvent être nécessaires pour configurer le SCIM depuis Okta IAM Identity Center.

Avant de commencer

Avant de configurer le provisionnement SCIM entre Okta et IAM Identity Center, nous vous recommandons de procéder à un premier examen. Considérations relatives à l'utilisation du provisionnement automatique

Vérifiez les éléments suivants avant de commencer :

- Chaque Okta utilisateur doit avoir un prénom, un nom de famille, un nom d'utilisateur et une valeur de nom d'affichage spécifiés.
- Chaque Okta utilisateur ne dispose que d'une seule valeur par attribut de données, tel qu'une adresse e-mail ou un numéro de téléphone. Les utilisateurs possédant plusieurs valeurs ne parviendront pas à se synchroniser. Si certains utilisateurs ont plusieurs valeurs dans leurs attributs, supprimez les attributs dupliqués avant de tenter de configurer l'utilisateur dans IAM Identity Center. Par exemple, un seul attribut de numéro de téléphone peut être synchronisé, étant donné que l'attribut de numéro de téléphone par défaut est « téléphone professionnel », utilisez l'attribut « téléphone professionnel » pour stocker le numéro de téléphone de l'utilisateur, même si le numéro de téléphone de l'utilisateur est un téléphone fixe ou un téléphone mobile.

- Si vous mettez à jour l'adresse d'un utilisateur, vous devez spécifier StreetAddress, city, state, ZipCode et CountryCode. Si aucune de ces valeurs n'est spécifiée pour l'Oktautilisateur au moment de la synchronisation, l'utilisateur (ou les modifications apportées à l'utilisateur) ne seront pas provisionnés.

> **Note**
>
> Les droits et les attributs de rôle ne sont pas pris en charge et ne peuvent pas être synchronisés avec IAM Identity Center.
> L'utilisation du même Okta groupe pour les devoirs et le transfert de groupe n'est actuellement pas prise en charge. Pour maintenir des appartenances de groupe cohérentes entre IAM Identity Center Okta et IAM Identity Center, créez un groupe distinct et configurez-le pour transférer des groupes vers IAM Identity Center.

Étape 1 : obtenir les métadonnées SAML depuis votre compte Okta

1. Connectez-vous auOkta admin dashboard, développez Applications, puis sélectionnez Applications.
2. Sur la page Applications, choisissez Browse App Catalog (Parcourir le catalogue d'applications).
3. Dans le champ de recherche, tapez AWS IAM Identity Center, sélectionnez l'application pour ajouter l'application IAM Identity Center.
4. Sélectionnez l'onglet Se connecter.
5. Sous Certificats de signature SAML, sélectionnez Actions, puis Afficher les métadonnées IdP. Un nouvel onglet de navigateur s'ouvre et affiche l'arborescence du document d'un fichier XML. Sélectionnez tout le code XML de `<md:EntityDescriptor>` à `</md:EntityDescriptor>` et copiez-le dans un fichier texte.
6. Enregistrez le fichier texte sous`metadata.xml`.

Laissez la console Okta admin dashboard ouverte, vous continuerez à utiliser cette console dans les étapes ultérieures.

Étape 2 : Configuration Okta en tant que source d'identité pour IAM Identity Center

1. Ouvrez la console IAM Identity Center en tant qu'utilisateur doté de privilèges administratifs.
2. Choisissez Paramètres dans le volet de navigation de gauche.

3. Sur la page Paramètres, choisissez Actions, puis Modifier la source d'identité.
4. Sous Choisir une source d'identité, sélectionnez Fournisseur d'identité externe, puis cliquez sur Suivant.
5. Sous Configurer le fournisseur d'identité externe, procédez comme suit :

   a. Sous Métadonnées du fournisseur de services, choisissez Télécharger le fichier de métadonnées pour télécharger le fichier de métadonnées IAM Identity Center et l'enregistrer sur votre système. Vous fournirez le fichier de métadonnées SAML d'IAM Identity Center Okta ultérieurement dans ce didacticiel.

      Copiez les éléments suivants dans un fichier texte pour y accéder facilement :

      - URL du service client d'assertion (ACS) du centre d'identité IAM
      - URL de l'émetteur du IAM Identity Center

      Vous aurez besoin de ces valeurs plus loin dans ce didacticiel.

   b. Sous Métadonnées du fournisseur d'identité, sous Méta IDP SAML, sélectionnez Choisir un fichier, puis sélectionnez le `metadata.xml` fichier que vous avez créé à l'étape précédente.

   c. Choisissez Suivant.
6. Une fois que vous avez lu la clause de non-responsabilité et que vous êtes prêt à continuer, entrez ACCEPT.
7. Choisissez Modifier la source d'identité.

   Laissez la AWS console ouverte, vous continuerez à l'utiliser à l'étape suivante.
8. Revenez à l'onglet Connexion de l' AWS IAM Identity Center application Okta admin dashboard et sélectionnez-le, puis cliquez sur Modifier.
9. Dans Paramètres de connexion avancés, entrez les informations suivantes :

   - Pour l'URL ACS, entrez la valeur que vous avez copiée pour l'URL IAM Identity Center Assertion Consumer Service (ACS)
   - Pour URL de l'émetteur, entrez la valeur que vous avez copiée pour l'URL de l'émetteur d'IAM Identity Center
   - Pour le format du nom d'utilisateur de l'application, sélectionnez l'une des options du menu déroulant.

Assurez-vous que la valeur que vous choisissez est unique pour chaque utilisateur. Pour ce didacticiel, sélectionnez le nom d'utilisateur Okta

10. Choisissez Enregistrer.

Vous êtes maintenant prêt à approvisionner les utilisateurs depuis Okta IAM Identity Center. Laissez le champ Okta admin dashboard ouvert et revenez à la console IAM Identity Center pour passer à l'étape suivante.

Étape 3 : Pour approvisionner les utilisateurs depuis Okta

1. Dans la console IAM Identity Center, sur la page Paramètres, recherchez la zone Informations de provisionnement automatique, puis choisissez Activer. Cela permet le provisionnement automatique dans IAM Identity Center et affiche les informations nécessaires sur le point de terminaison SCIM et le jeton d'accès.
2. Dans la boîte de dialogue de provisionnement automatique entrant, copiez chacune des valeurs des options suivantes :

   - Point de terminaison SCIM
   - Jeton d'accès

   Plus loin dans ce didacticiel, vous saisirez ces valeurs pour configurer le provisionnement. Okta
3. Choisissez Fermer.
4. Retournez à l'application IAM Identity Center Okta admin dashboard et naviguez vers celle-ci.
5. Sur la page de l'application IAM Identity Center, choisissez l'onglet Provisioning, puis dans le menu de navigation de gauche, sous Paramètres, choisissez Integration.
6. Choisissez Modifier, puis cochez la case à côté de Activer l'intégration des API pour activer le provisionnement.
7. Configurez Okta avec les valeurs de provisionnement SCIM provenant d'IAM Identity Center que vous avez copiées plus tôt dans ce didacticiel :

   a. Dans le champ URL de base, entrez la valeur du point de terminaison SCIM. Assurez-vous de supprimer la barre oblique à la fin de l'URL.

   b. Dans le champ API Token, entrez la valeur du jeton d'accès.

8. Choisissez Test API Credentials pour vérifier que les informations d'identification saisies sont valides.

   Le message AWS IAM Identity Center a été vérifié avec succès ! écrans.

9. Choisissez Enregistrer. Vous êtes dirigé vers la zone Paramètres, avec l'option Intégration sélectionnée.
10. Sous Paramètres, choisissez Vers l'application, puis cochez la case Activer pour chacune des fonctionnalités de provisionnement vers l'application que vous souhaitez activer. Pour ce didacticiel, sélectionnez toutes les options.
11. Choisissez Enregistrer.

Vous êtes maintenant prêt à synchroniser vos utilisateurs depuis Okta IAM Identity Center.

Étape 4 : Synchroniser les utilisateurs depuis Okta IAM Identity Center

Par défaut, aucun groupe ou utilisateur n'est attribué à votre application Okta IAM Identity Center. Les groupes de provisionnement provisionnent les utilisateurs membres du groupe. Procédez comme suit pour synchroniser les groupes et les utilisateurs avec IAM Identity Center.

1. Sur la page de l'application Okta IAM Identity Center, choisissez l'onglet Assignments. Vous pouvez attribuer à la fois des personnes et des groupes à l'application IAM Identity Center.

   a. Pour affecter des personnes :

      - Sur la page Attributions, choisissez Attribuer, puis Attribuer à des personnes.
      - Choisissez les Okta utilisateurs auxquels vous souhaitez avoir accès à l'application IAM Identity Center. Choisissez Attribuer, puis Enregistrer et revenir en arrière, puis cliquez sur Terminé.

      Cela lance le processus de mise en service des utilisateurs dans IAM Identity Center.

   b. Pour attribuer des groupes :

      - Sur la page Attributions, choisissez Attribuer, puis Attribuer aux groupes.
      - Choisissez les Okta groupes auxquels vous souhaitez avoir accès à l'application IAM Identity Center. Choisissez Attribuer, puis Enregistrer et revenir en arrière, puis cliquez sur Terminé.

Cela lance le processus de mise en service des utilisateurs du groupe dans IAM Identity Center.

> **Note**
>
> Vous devrez peut-être spécifier des attributs supplémentaires pour le groupe s'ils ne figurent pas dans tous les enregistrements utilisateur. Les attributs spécifiés pour le groupe remplaceront toute valeur d'attribut individuelle.

2. Choisissez l'onglet Push Groups. Choisissez le Okta groupe qui contient tous les groupes que vous avez attribués à l'application IAM Identity Center. Choisissez Enregistrer.

   Le statut du groupe passe à Actif une fois que le groupe et ses membres ont été transférés vers IAM Identity Center.

3. Retournez à l'onglet Affectations.

4. Si certains de vos utilisateurs ne sont pas membres des groupes que vous avez transférés vers IAM Identity Center, ajoutez-les individuellement en procédant comme suit :

   Sur la page Attributions, choisissez Attribuer, puis Attribuer à des personnes.

5. Choisissez les Okta utilisateurs auxquels vous souhaitez avoir accès à l'application IAM Identity Center. Choisissez Attribuer, puis Enregistrer et revenir en arrière, puis cliquez sur Terminé.

   Cela lance le processus de mise en service des utilisateurs individuels dans IAM Identity Center.

   > **Note**
   >
   > Vous pouvez également attribuer des utilisateurs et des groupes à l' AWS IAM Identity Center application, depuis la page Applications duOkta admin dashboard. Pour ce faire, sélectionnez l'icône Paramètres, puis choisissez Attribuer aux utilisateurs ou Attribuer aux groupes, puis spécifiez l'utilisateur ou le groupe.

6. Retournez à la console IAM Identity Center. Dans le volet de navigation de gauche, sélectionnez Utilisateurs. Vous devriez voir la liste des utilisateurs renseignée par vos Okta utilisateurs.

Félicitations !

Vous avez correctement configuré une connexion SAML entre Okta et AWS et vous avez vérifié que le provisionnement automatique fonctionne. Vous pouvez désormais attribuer ces utilisateurs à des comptes et à des applications dans IAM Identity Center. Dans le cadre de ce didacticiel, à l'étape suivante, désignons l'un des utilisateurs comme administrateur du centre d'identité IAM en lui accordant des autorisations administratives sur le compte de gestion.

Étape 5 : Accorder Okta aux utilisateurs l'accès aux comptes

1. Dans le volet de navigation d'IAM Identity Center, sous Autorisations multi-comptes, sélectionnez. Comptes AWS
2. Sur la Comptes AWSpage, la structure organisationnelle affiche la racine de votre organisation avec vos comptes en dessous dans la hiérarchie. Cochez la case correspondant à votre compte de gestion, puis sélectionnez Attribuer des utilisateurs ou des groupes.
3. Le flux de travail Attribuer des utilisateurs et des groupes s'affiche. Il se compose de trois étapes :

   a. Pour l'étape 1 : Sélectionnez les utilisateurs et les groupes, choisissez l'utilisateur qui exécutera la fonction d'administrateur. Ensuite, sélectionnez Suivant.

   b. Pour l'étape 2 : Sélectionnez des ensembles d'autorisations, choisissez Créer un ensemble d'autorisations pour ouvrir un nouvel onglet qui vous indique les trois sous-étapes nécessaires à la création d'un ensemble d'autorisations.

      i. Pour l'étape 1 : Sélectionnez le type d'ensemble d'autorisations, procédez comme suit :

         - Dans Type d'ensemble d'autorisations, choisissez Ensemble d'autorisations prédéfini.
         - Dans Politique pour un ensemble d'autorisations prédéfini, sélectionnez AdministratorAccess.

         Choisissez Suivant.

      ii. Pour l'étape 2 : Spécifiez les détails de l'ensemble d'autorisations, conservez les paramètres par défaut et choisissez Next.

Les paramètres par défaut créent un ensemble d'autorisations nommé *AdministratorAccess*avec une durée de session fixée à une heure.

iii. Pour l'étape 3 : révision et création, vérifiez que le type d'ensemble d'autorisations utilise la politique AWS gérée AdministratorAccess. Choisissez Créer. Sur la page Ensembles d'autorisations, une notification apparaît pour vous informer que l'ensemble d'autorisations a été créé. Vous pouvez maintenant fermer cet onglet dans votre navigateur Web.

Dans l'onglet du navigateur Attribuer des utilisateurs et des groupes, vous êtes toujours à l'étape 2 : Sélectionnez les ensembles d'autorisations à partir desquels vous avez lancé le flux de travail de création d'ensembles d'autorisations.

Dans la zone Ensembles d'autorisations, cliquez sur le bouton Actualiser. L'ensemble *AdministratorAccess*d'autorisations que vous avez créé apparaît dans la liste. Cochez la case correspondant à cet ensemble d'autorisations, puis choisissez Next.

c. Pour l'étape 3 : vérifier et envoyer, passez en revue l'utilisateur et l'ensemble d'autorisations sélectionnés, puis choisissez Soumettre.

La page Compte AWS est mise à jour avec un message indiquant que vous êtes en cours de configuration. Patientez jusqu'à ce que le processus soit terminé.

Vous êtes renvoyé à la Comptes AWS page. Un message de notification vous informe que votre Compte AWS compte a été réapprovisionné et que l'ensemble d'autorisations mis à jour a été appliqué. Lorsque l'utilisateur se connecte, il a la possibilité de choisir le *AdministratorAccess*rôle.

> **Note**
>
> La synchronisation automatique SCIM depuis Okta ne prend en charge que le provisionnement des utilisateurs ; les groupes ne sont pas automatiquement provisionnés. Vous ne pouvez pas créer de groupes pour vos Okta utilisateurs à l'aide du AWS Management Console. Après avoir configuré les utilisateurs, vous pouvez créer des groupes à l'aide d'une CLI ou d'une opération d'API

Étape 6 : Confirmer l'accès Okta des utilisateurs aux AWS ressources

1. Connectez-vous à l'Okta dashboardaide d'un compte utilisateur de test.
2. Sous Mes applications, sélectionnez l'AWS IAM Identity Centericône.
3. Vous êtes connecté au portail et vous pouvez voir l' Compte AWS icône. Développez cette icône pour voir la liste des Comptes AWS objets auxquels l'utilisateur peut accéder. Dans ce didacticiel, vous n'avez travaillé qu'avec un seul compte. Par conséquent, l'extension de l'icône ne permet d'afficher qu'un seul compte.
4. Sélectionnez le compte pour afficher les ensembles d'autorisations disponibles pour l'utilisateur. Dans ce didacticiel, vous avez créé l'ensemble AdministratorAccessd'autorisations.
5. À côté de l'ensemble d'autorisations se trouvent des liens indiquant le type d'accès disponible pour cet ensemble d'autorisations. Lorsque vous avez créé l'ensemble d'autorisations, vous avez indiqué que la console de gestion et l'accès par programmation devaient être activés. Ces deux options sont donc présentes. Sélectionnez Console de gestion pour ouvrir le AWS Management Console.
6. L'utilisateur est connecté à la console.

(Facultatif) Transmission d'attributs pour le contrôle d'accès

Vous pouvez éventuellement utiliser la Attributs pour le contrôle d'accès fonctionnalité d'IAM Identity Center pour transmettre un `Attribute` élément dont l'`Name`attribut est défini sur. `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` Cet élément vous permet de transmettre des attributs en tant que balises de session dans l'assertion SAML. Pour plus d'informations sur les balises de session, consultez la section Transmission de balises de session AWS STS dans le guide de l'utilisateur IAM.

Pour transmettre des attributs en tant que balises de session, incluez l'élément `AttributeValue` qui spécifie la valeur de la balise. Par exemple, pour transmettre la paire clé-valeur du tag`CostCenter = blue`, utilisez l'attribut suivant.

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

Si vous devez ajouter plusieurs attributs, incluez un `Attribute` élément distinct pour chaque balise.

Étapes suivantes

Maintenant que vous avez configuré Okta en tant que fournisseur d'identité et que vous avez configuré les utilisateurs dans IAM Identity Center, vous pouvez :

- Accorder l'accès à Comptes AWS, voirAttribuer un accès utilisateur à Comptes AWS.
- Accordez l'accès aux applications cloud, voirAttribuer un accès utilisateur aux applications dans la console IAM Identity Center.
- Configurez les autorisations en fonction des fonctions du poste, voir Création d'un ensemble d'autorisations

Configuration du provisionnement SCIM entre OneLogin et IAM Identity Center

IAM Identity Center prend en charge le provisionnement automatique (synchronisation) des informations sur les utilisateurs et les groupes depuis OneLogin IAM Identity Center à l'aide du protocole SCIM (System for Cross-domain Identity Management) v2.0. Vous configurez cette connexion en OneLogin utilisant votre point de terminaison SCIM pour IAM Identity Center et un jeton porteur créé automatiquement par IAM Identity Center. Lorsque vous configurez la synchronisation SCIM, vous créez un mappage de vos attributs utilisateur avec OneLogin les attributs nommés dans IAM Identity Center. Cela entraîne la correspondance des attributs attendus entre IAM Identity Center etOneLogin.

Les étapes suivantes vous expliquent comment activer le provisionnement automatique des utilisateurs et des groupes depuis IAM Identity Center OneLogin à l'aide du protocole SCIM.

> **Note**
>
> Avant de commencer à déployer SCIM, nous vous recommandons de consulter d'abord leConsidérations relatives à l'utilisation du provisionnement automatique.

Rubriques

- Prérequis
- Étape 1 : activer le provisionnement dans IAM Identity Center

Prérequis

Vous aurez besoin des éléments suivants avant de pouvoir commencer :

- Un OneLogin compte. Si vous n'avez pas de compte existant, vous pourrez peut-être obtenir un essai gratuit ou un compte développeur sur le OneLoginsite Web.
- Un compte compatible avec IAM Identity Center (gratuit). Pour plus d'informations, voir Activer le centre d'identité IAM.
- Une connexion SAML entre votre OneLogin compte et IAM Identity Center. Pour plus d'informations, consultez la section Activation de l'authentification unique entre OneLogin et AWS sur le blog du réseau de AWS partenaires.

Étape 1 : activer le provisionnement dans IAM Identity Center

Dans cette première étape, vous utilisez la console IAM Identity Center pour activer le provisionnement automatique.

Pour activer le provisionnement automatique dans IAM Identity Center

1. Une fois que vous avez rempli les conditions requises, ouvrez la console IAM Identity Center.
2. Choisissez Paramètres dans le volet de navigation de gauche.
3. Sur la page Paramètres, recherchez la zone Informations de provisionnement automatique, puis choisissez Activer. Cela active immédiatement le provisionnement automatique dans IAM Identity Center et affiche les informations nécessaires sur le point de terminaison SCIM et le jeton d'accès.
4. Dans la boîte de dialogue de provisionnement automatique entrant, copiez chacune des valeurs des options suivantes. Vous devrez les coller ultérieurement lorsque vous configurerez le provisionnement dans votre IdP.

    a. Point de terminaison SCIM

b. Jeton d'accès

5. Choisissez Fermer.

Vous avez maintenant configuré le provisionnement dans la console IAM Identity Center. Vous devez maintenant effectuer les tâches restantes à l'aide de la console OneLogin d'administration, comme décrit dans la procédure suivante.

Étape 2 : configurer le provisionnement dans OneLogin

Utilisez la procédure suivante dans la console OneLogin d'administration pour activer l'intégration entre IAM Identity Center et l'application IAM Identity Center. Cette procédure suppose que vous avez déjà configuré l'application AWS Single Sign-On OneLogin pour l'authentification SAML. Si vous n'avez pas encore créé cette connexion SAML, veuillez le faire avant de continuer, puis revenez ici pour terminer le processus de provisionnement SCIM. Pour plus d'informations sur la configuration de SAML avecOneLogin, consultez la section Activation de l'authentification unique entre OneLogin et AWS sur le blog du réseau de AWS partenaires.

Pour configurer le provisionnement dans OneLogin

1. Connectez-vous àOneLogin, puis accédez à Applications > Applications.
2. Sur la page Applications, recherchez l'application que vous avez créée précédemment pour établir votre connexion SAML avec IAM Identity Center. Choisissez-le, puis sélectionnez Configuration dans la barre de navigation de gauche.
3. Dans la procédure précédente, vous avez copié la valeur du point de terminaison SCIM dans IAM Identity Center. Collez cette valeur dans le champ URL de base SCIM dansOneLogin. Assurez-vous de supprimer la barre oblique à la fin de l'URL. Dans la procédure précédente, vous avez également copié la valeur du jeton d'accès dans IAM Identity Center. Collez cette valeur dans le champ SCIM Bearer Token. OneLogin
4. À côté de Connexion API, cliquez sur Activer, puis sur Enregistrer pour terminer la configuration.
5. Dans la barre de navigation de gauche, choisissez Provisioning.
6. Cochez les cases Activer le provisionnement, Créer un utilisateur, Supprimer un utilisateur et Mettre à jour un utilisateur, puis choisissez Enregistrer.
7. Dans la barre de navigation de gauche, sélectionnez Utilisateurs.
8. Cliquez sur Autres actions et choisissez Synchroniser les connexions. Vous devriez recevoir le message Synchronisation des utilisateurs avec l'authentification AWS unique.

9. Cliquez à nouveau sur Autres actions, puis choisissez Réappliquer les mappages d'autorisations. Vous devriez recevoir le message Les mappages sont réappliqués.
10. À ce stade, le processus de provisionnement doit commencer. Pour le confirmer, accédez à Activité > Événements et surveillez la progression. Les événements de provisionnement réussis, ainsi que les erreurs, doivent apparaître dans le flux d'événements.
11. Pour vérifier que vos utilisateurs et groupes ont tous été correctement synchronisés avec IAM Identity Center, revenez à la console IAM Identity Center et sélectionnez Utilisateurs. Vos utilisateurs synchronisés OneLogin apparaissent sur la page Utilisateurs. Vous pouvez également consulter vos groupes synchronisés sur la page Groupes.
12. Pour synchroniser automatiquement les modifications des utilisateurs avec IAM Identity Center, accédez à la page Provisioning, recherchez la section Exiger l'approbation de l'administrateur avant que cette action ne soit effectuée, désélectionnez Créer un utilisateur, Supprimer un utilisateur et/ou Mettre à jour un utilisateur, puis cliquez sur Enregistrer.

(Facultatif) Étape 3 : Configuration des attributs utilisateur OneLogin pour le contrôle d'accès dans IAM Identity Center

Il s'agit d'une procédure facultative OneLogin si vous choisissez de configurer les attributs que vous utiliserez dans IAM Identity Center pour gérer l'accès à vos AWS ressources. Les attributs que vous définissez OneLogin sont transmis dans une assertion SAML à IAM Identity Center. Vous allez ensuite créer un ensemble d'autorisations dans IAM Identity Center pour gérer l'accès en fonction des attributs que vous avez transmisOneLogin.

Avant de commencer cette procédure, vous devez d'abord activer la Attributs pour le contrôle d'accès fonctionnalité. Pour plus d'informations sur cette étape, consultez Activer et configurer les attributs pour le contrôle d'accès.

Pour configurer les attributs utilisateur OneLogin pour le contrôle d'accès dans IAM Identity Center

1. Connectez-vous àOneLogin, puis accédez à Applications > Applications.
2. Sur la page Applications, recherchez l'application que vous avez créée précédemment pour établir votre connexion SAML avec IAM Identity Center. Sélectionnez-le, puis sélectionnez Paramètres dans la barre de navigation de gauche.
3. Dans la section Paramètres requis, procédez comme suit pour chaque attribut que vous souhaitez utiliser dans IAM Identity Center :

a. Choisissez +.

b. Dans Nom du champhttps://aws.amazon.com/SAML/Attributes/AccessControl:**AttributeName**, entrez et remplacez **AttributeName** par le nom de l'attribut que vous attendez dans IAM Identity Center. Par exemple, https://aws.amazon.com/SAML/Attributes/AccessControl:**Department**.

c. Sous Drapeaux, cochez la case à côté de Inclure dans l'assertion SAML, puis choisissez Enregistrer.

d. Dans le champ Valeur, utilisez la liste déroulante pour choisir les attributs OneLogin utilisateur. Par exemple, Department.

4. Choisissez Enregistrer.

(Facultatif) Transmission d'attributs pour le contrôle d'accès

Vous pouvez éventuellement utiliser la Attributs pour le contrôle d'accès fonctionnalité d'IAM Identity Center pour transmettre un Attribute élément dont l'Nameattribut est défini sur. https://aws.amazon.com/SAML/Attributes/AccessControl:**{TagKey}** Cet élément vous permet de transmettre des attributs en tant que balises de session dans l'assertion SAML. Pour plus d'informations sur les balises de session, consultez la section Transmission de balises de session AWS STS dans le guide de l'utilisateur IAM.

Pour transmettre des attributs en tant que balises de session, incluez l'élément AttributeValue qui spécifie la valeur de la balise. Par exemple, pour transmettre la paire clé-valeur du tagCostCenter = blue, utilisez l'attribut suivant.

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

Si vous devez ajouter plusieurs attributs, incluez un Attribute élément distinct pour chaque balise.

Résolution des problèmes

Les informations suivantes peuvent vous aider à résoudre certains problèmes courants que vous pouvez rencontrer lors de la configuration du provisionnement automatique avec. OneLogin

Les groupes ne sont pas fournis à IAM Identity Center

Par défaut, les groupes ne peuvent pas être approvisionnés depuis OneLogin IAM Identity Center. Assurez-vous d'avoir activé le provisionnement de groupe pour votre application IAM Identity Center dans. OneLogin Pour ce faire, connectez-vous à la console OneLogin d'administration et assurez-vous que l'option Inclure dans le provisionnement utilisateur est sélectionnée dans les propriétés de l'application IAM Identity Center (application IAM Identity Center > Paramètres > Groupes). Pour plus de détails sur la création de groupes dansOneLogin, notamment sur la synchronisation des OneLogin rôles en tant que groupes dans SCIM, consultez le OneLoginsite Web.

Rien n'est synchronisé depuis OneLogin IAM Identity Center, même si tous les paramètres sont corrects

Outre la remarque ci-dessus concernant l'approbation de l'administrateur, vous devrez réappliquer les mappages de droits pour que de nombreuses modifications de configuration prennent effet. Vous pouvez le trouver dans Applications > Applications > Application IAM Identity Center > Autres actions. Vous pouvez consulter les détails et les journaux de la plupart des actionsOneLogin, y compris les événements de synchronisation, sous Activité > Événements.

J'ai supprimé ou désactivé un groupe dansOneLogin, mais il apparaît toujours dans IAM Identity Center

OneLoginne prend actuellement pas en charge l'opération SCIM DELETE pour les groupes, ce qui signifie que le groupe continue d'exister dans IAM Identity Center. Vous devez donc supprimer le groupe directement d'IAM Identity Center pour vous assurer que toutes les autorisations correspondantes dans IAM Identity Center pour ce groupe sont supprimées.

J'ai supprimé un groupe dans IAM Identity Center sans le supprimer au préalable OneLogin et je rencontre maintenant des problèmes de synchronisation entre les utilisateurs et les groupes

Pour remédier à cette situation, assurez-vous d'abord que vous ne disposez pas de règles ou de configurations de provisionnement de groupe redondantes. OneLogin Par exemple, un groupe directement affecté à une application ainsi qu'une règle qui publie pour le même groupe. Supprimez ensuite tous les groupes indésirables dans IAM Identity Center. EnfinOneLogin, actualisez les droits (application IAM Identity Center > Provisioning > Droits), puis réappliquez les mappages de droits (application IAM Identity Center > Autres actions). Pour éviter ce problème à l'avenir, effectuez d'abord la modification pour arrêter le provisionnement du groupeOneLogin, puis supprimez le groupe d'IAM Identity Center.

Utilisation de Ping Identity produits avec IAM Identity Center

Les Ping Identity produits suivants ont été testés avec IAM Identity Center.

Rubriques

PingFederate

IAM Identity Center prend en charge le provisionnement automatique (synchronisation) des informations sur les utilisateurs et les groupes depuis le PingFederate produit Ping Identity (ci-après « Ping ») dans IAM Identity Center. Ce provisionnement utilise le protocole SCIM (System for Cross-Domain Identity Management) v2.0. Vous configurez cette connexion à PingFederate l'aide de votre point de terminaison SCIM et de votre jeton d'accès IAM Identity Center. Lorsque vous configurez la synchronisation SCIM, vous créez un mappage de vos attributs utilisateur avec PingFederate les attributs nommés dans IAM Identity Center. Cela entraîne la correspondance des attributs attendus entre IAM Identity Center etPingFederate.

Ce guide est basé sur la PingFederate version 10.2. Les étapes pour les autres versions peuvent varier. Contactez-nous Ping pour plus d'informations sur la configuration du provisionnement vers IAM Identity Center pour les autres versions de. PingFederate

Les étapes suivantes vous expliquent comment activer le provisionnement automatique des utilisateurs et des groupes depuis IAM Identity Center PingFederate à l'aide du protocole SCIM.

> **Note**
>
> Avant de commencer à déployer SCIM, nous vous recommandons de consulter d'abord leConsidérations relatives à l'utilisation du provisionnement automatique. Passez ensuite en revue les autres considérations dans la section suivante.

Rubriques

- Étape 1 : activer le provisionnement dans IAM Identity Center
- Étape 2 : configurer le provisionnement dans PingFederate
- (Facultatif) Étape 3 : configurer les attributs utilisateur dans PingFed erate pour le contrôle d'accès dans IAM Identity Center
- (Facultatif) Transmission d'attributs pour le contrôle d'accès

Prérequis

Vous aurez besoin des éléments suivants avant de pouvoir commencer :

- Un PingFederate serveur en état de marche. Si vous n'avez pas de PingFederate serveur existant, vous pourrez peut-être obtenir un essai gratuit ou un compte développeur sur le site Web de Ping Identity. La version d'essai inclut le téléchargement de licences et de logiciels ainsi que la documentation associée.
- Une copie du logiciel PingFederate IAM Identity Center Connector installé sur votre PingFederate serveur. Pour plus d'informations sur la façon d'obtenir ce logiciel, consultez la section IAM Identity Center Connector sur le ing Identity site Web de P.
- Un compte compatible avec IAM Identity Center (gratuit). Pour plus d'informations, consultez la section Activer le centre d'identité IAM.
- Une connexion SAML entre votre PingFederate instance et IAM Identity Center. Pour obtenir des instructions sur la configuration de cette connexion, consultez la PingFederate documentation. En résumé, il est recommandé d'utiliser le connecteur IAM Identity Center pour configurer le « Browser SSO » dansPingFederate, en utilisant les fonctionnalités de « téléchargement » et d' « importation » de métadonnées situées aux deux extrémités pour échanger des métadonnées SAML entre IAM Identity Center PingFederate et IAM Identity Center.

Considérations supplémentaires

Les considérations suivantes sont importantes et peuvent avoir une incidence sur PingFederate la manière dont vous implémentez le provisionnement avec IAM Identity Center.

- Si un attribut (tel qu'un numéro de téléphone) est supprimé d'un utilisateur dans le magasin de données configuré dansPingFederate, cet attribut ne sera pas supprimé de l'utilisateur correspondant dans IAM Identity Center. Il s'agit d'une limitation connue dans la mise en PingFederate’s œuvre du fournisseur. Si un attribut est remplacé par une valeur différente (non vide) pour un utilisateur, cette modification sera synchronisée avec IAM Identity Center.

Étape 1 : activer le provisionnement dans IAM Identity Center

Dans cette première étape, vous utilisez la console IAM Identity Center pour activer le provisionnement automatique.

Pour activer le provisionnement automatique dans IAM Identity Center

1. Une fois que vous avez rempli les conditions requises, ouvrez la console IAM Identity Center.
2. Choisissez Paramètres dans le volet de navigation de gauche.
3. Sur la page Paramètres, recherchez la zone Informations de provisionnement automatique, puis choisissez Activer. Cela active immédiatement le provisionnement automatique dans IAM Identity Center et affiche les informations nécessaires sur le point de terminaison SCIM et le jeton d'accès.
4. Dans la boîte de dialogue de provisionnement automatique entrant, copiez chacune des valeurs des options suivantes. Vous devrez les coller ultérieurement lorsque vous configurerez le provisionnement dans votre IdP.
   a. Point de terminaison SCIM
   b. Jeton d'accès
5. Choisissez Fermer.

Maintenant que vous avez configuré le provisionnement dans la console IAM Identity Center, vous devez effectuer les tâches restantes à l'aide de la console d'PingFederateadministration. Les étapes sont décrites dans la procédure suivante.

Étape 2 : configurer le provisionnement dans PingFederate

Utilisez la procédure suivante dans la console d'PingFederateadministration pour activer l'intégration entre IAM Identity Center et le connecteur IAM Identity Center. Cette procédure suppose que vous avez déjà installé le logiciel IAM Identity Center Connector. Si vous ne l'avez pas encore fait, reportez-vous à cette procédurePrérequis, puis exécutez-la pour configurer le provisionnement SCIM.

> **Important**
>
> Si votre PingFederate serveur n'a pas encore été configuré pour le provisionnement SCIM sortant, vous devrez peut-être modifier le fichier de configuration pour activer le provisionnement. Pour plus d'informations, consultez Ping la documentation. En résumé,

vous devez modifier le `pf.provisioner.mode` paramètre du pingfederate-<version>/pingfederate/bin/run.propertiesfichier à une valeur autre que `OFF` (valeur par défaut) et redémarrer le serveur s'il est en cours d'exécution. Par exemple, vous pouvez choisir de l'utiliser `STANDALONE` si vous ne disposez pas actuellement d'une configuration haute disponibilité avecPingFederate.

Pour configurer le provisionnement dans PingFederate

1. Connectez-vous à la console PingFederate d'administration.
2. Sélectionnez Applications en haut de la page, puis cliquez sur SP Connections.
3. Localisez l'application que vous avez créée précédemment pour établir votre connexion SAML avec IAM Identity Center, puis cliquez sur le nom de la connexion.
4. Sélectionnez le type de connexion dans les en-têtes de navigation sombres situés en haut de la page. Vous devriez voir que l'authentification unique du navigateur est déjà sélectionnée dans votre configuration précédente de SAML. Si ce n'est pas le cas, vous devez d'abord suivre ces étapes avant de pouvoir continuer.
5. Cochez la case Outbound Provisioning, choisissez le type IAM Identity Center Cloud Connector, puis cliquez sur Enregistrer. Si le connecteur IAM Identity Center Cloud n'apparaît pas en option, assurez-vous d'avoir installé le connecteur IAM Identity Center et redémarré votre serveur. PingFederate
6. Cliquez sur Suivant à plusieurs reprises jusqu'à ce que vous arriviez sur la page de provisionnement sortant, puis cliquez sur le bouton Configurer le provisionnement.
7. Dans la procédure précédente, vous avez copié la valeur du point de terminaison SCIM dans IAM Identity Center. Collez cette valeur dans le champ URL SCIM de la PingFederate console. Assurez-vous de supprimer la barre oblique à la fin de l'URL. Dans la procédure précédente, vous avez également copié la valeur du jeton d'accès dans IAM Identity Center. Collez cette valeur dans le champ Access Token de la PingFederate console. Cliquez sur Sauvegarder
8. Sur la page Configuration des canaux (Configurer les canaux), cliquez sur Créer.
9. Entrez un nom de canal pour ce nouveau canal de provisionnement (tel que**`AWSIAMIdentityCenterchannel`**), puis cliquez sur Suivant.
10. Sur la page Source, choisissez le magasin de données actif que vous souhaitez utiliser pour votre connexion à IAM Identity Center, puis cliquez sur Suivant.

> **Note**
>
> Si vous n'avez pas encore configuré de source de données, vous devez le faire maintenant. Consultez la documentation Ping du produit pour savoir comment choisir et configurer une source de données dansPingFederate.

11. Sur la page Paramètres source, vérifiez que toutes les valeurs sont correctes pour votre installation, puis cliquez sur Suivant.
12. Sur la page Emplacement de la source, entrez les paramètres appropriés à votre source de données, puis cliquez sur Suivant. Par exemple, si vous utilisez Active Directory comme annuaire LDAP :
    a. Entrez le DN de base de votre forêt AD (tel que**`DC=myforest,DC=mydomain,DC=com`**).
    b. Dans Utilisateurs **>** Nom distinctif du groupe, spécifiez un groupe unique contenant tous les utilisateurs que vous souhaitez attribuer à IAM Identity Center. Si aucun groupe unique de ce type n'existe, créez-le dans AD, revenez à ce paramètre, puis entrez le DN correspondant.
    c. Spécifiez si vous souhaitez rechercher des sous-groupes (recherche imbriquée) et indiquez tout filtre LDAP requis.
    d. Dans Groupes **>** Nom du groupe, spécifiez un groupe unique contenant tous les groupes que vous souhaitez attribuer à IAM Identity Center. Dans de nombreux cas, il peut s'agir du même DN que celui que vous avez spécifié dans la section Utilisateurs. Entrez les valeurs de recherche et de filtre imbriquées selon les besoins.
13. Sur la page Mappage des attributs, vérifiez les points suivants, puis cliquez sur Suivant :
    a. Le champ UserName doit être mappé à un attribut au format e-mail (user@domain.com). Elle doit également correspondre à la valeur que l'utilisateur utilisera pour se connecter à Ping. Cette valeur est à son tour renseignée dans la `nameId` réclamation SAML lors de l'authentification fédérée et utilisée pour établir une correspondance avec l'utilisateur dans IAM Identity Center. Par exemple, lorsque vous utilisez Active Directory, vous pouvez choisir de le spécifier `UserPrincipalName` comme UserName.
    b. Les autres champs marqués d'un * doivent être mappés à des attributs non nuls pour vos utilisateurs.
14. Sur la page Activation et résumé, définissez le statut du canal sur Actif pour que la synchronisation démarre immédiatement après l'enregistrement de la configuration.

15. Vérifiez que toutes les valeurs de configuration de la page sont correctes, puis cliquez sur Terminé.
16. Sur la page Gérer les chaînes, cliquez sur Enregistrer.
17. À ce stade, le provisionnement commence. Pour confirmer l'activité, vous pouvez consulter le fichier provisioner.log, situé par défaut dans le pingfederate-<version>/pingfederate/logrépertoire de votre PingFederate serveur.
18. Pour vérifier que les utilisateurs et les groupes ont été correctement synchronisés avec IAM Identity Center, revenez à la console IAM Identity Center et sélectionnez Utilisateurs. Les utilisateurs synchronisés PingFederate apparaissent sur la page Utilisateurs. Vous pouvez également consulter les groupes synchronisés sur la page Groupes.

(Facultatif) Étape 3 : configurer les attributs utilisateur dans PingFed erate pour le contrôle d'accès dans IAM Identity Center

Il s'agit d'une procédure facultative PingFederate si vous choisissez de configurer les attributs que vous utiliserez dans IAM Identity Center pour gérer l'accès à vos AWS ressources. Les attributs que vous définissez PingFederate sont transmis dans une assertion SAML à IAM Identity Center. Vous allez ensuite créer un ensemble d'autorisations dans IAM Identity Center pour gérer l'accès en fonction des attributs que vous avez transmisPingFederate.

Avant de commencer cette procédure, vous devez d'abord activer la Attributs pour le contrôle d'accès fonctionnalité. Pour plus d'informations sur cette étape, consultez Activer et configurer les attributs pour le contrôle d'accès.

Pour configurer les attributs utilisateur PingFederate pour le contrôle d'accès dans IAM Identity Center

1. Connectez-vous à la console PingFederate d'administration.
2. Choisissez Applications en haut de la page, puis cliquez sur SP Connections.
3. Localisez l'application que vous avez créée précédemment pour établir votre connexion SAML avec IAM Identity Center, puis cliquez sur le nom de la connexion.
4. Choisissez Browser SSO dans les en-têtes de navigation sombres situés en haut de la page. Cliquez ensuite sur Configurer le SSO du navigateur.
5. Sur la page Configurer l'authentification unique du navigateur, choisissez Création d'assertions, puis cliquez sur Configurer la création d'assertions.
6. Sur la page Configurer la création d'assertions, sélectionnez Attribute Contract.

7. Sur la page Contrat d'attribut, sous la section Étendre le contrat, ajoutez un nouvel attribut en effectuant les étapes suivantes :

   a. Dans la zone de texte, entrez`https://aws.amazon.com/SAML/Attributes/AccessControl:`**`AttributeName`**, remplacez **`AttributeName`** par le nom de l'attribut que vous attendez dans IAM Identity Center. Par exemple, `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Department`**.

   b. Pour Format du nom d'attribut, sélectionnez urn:oasis:names:tc:SAML:2.0:attrname-format:uri.

   c. Choisissez Ajouter, puis Next.

8. Sur la page Mappage des sources d'authentification, choisissez l'instance d'adaptateur configurée avec votre application.

9. Sur la page Exécution du contrat d'attribut, choisissez la source (magasin de données) et la valeur (attribut du magasin de données) pour le contrat d'attribut`https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Department`**.

   > **Note**
   >
   > Si vous n'avez pas encore configuré de source de données, vous devez le faire maintenant. Consultez la documentation Ping du produit pour savoir comment choisir et configurer une source de données dansPingFederate.

10. Cliquez sur Suivant à plusieurs reprises jusqu'à ce que vous arriviez sur la page Activation et résumé, puis cliquez sur Enregistrer.

(Facultatif) Transmission d'attributs pour le contrôle d'accès

Vous pouvez éventuellement utiliser la Attributs pour le contrôle d'accès fonctionnalité d'IAM Identity Center pour transmettre un `Attribute` élément dont l'`Name`attribut est défini sur. `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`** Cet élément vous permet de transmettre des attributs en tant que balises de session dans l'assertion SAML. Pour plus d'informations sur les balises de session, consultez la section Transmission de balises de session AWS STS dans le guide de l'utilisateur IAM.

Pour transmettre des attributs en tant que balises de session, incluez l'élément `AttributeValue` qui spécifie la valeur de la balise. Par exemple, pour transmettre la paire clé-valeur du tag`CostCenter = blue`, utilisez l'attribut suivant.

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

Si vous devez ajouter plusieurs attributs, incluez un `Attribute` élément distinct pour chaque balise.

PingOne

IAM Identity Center prend en charge le provisionnement automatique (synchronisation) des informations utilisateur depuis le PingOne produit Ping Identity (ci-après « Ping ») vers IAM Identity Center. Ce provisionnement utilise le protocole SCIM (System for Cross-Domain Identity Management) v2.0. Vous configurez cette connexion à PingOne l'aide de votre point de terminaison SCIM et de votre jeton d'accès IAM Identity Center. Lorsque vous configurez la synchronisation SCIM, vous créez un mappage de vos attributs utilisateur avec PingOne les attributs nommés dans IAM Identity Center. Cela entraîne la correspondance des attributs attendus entre IAM Identity Center etPingOne.

Ce guide est basé sur PingOne la version d'octobre 2020. Les étapes à suivre pour les nouvelles versions peuvent varier. Contactez-nous Ping pour plus d'informations sur la configuration du provisionnement vers IAM Identity Center pour les autres versions de. PingOne Ce guide contient également quelques remarques concernant la configuration de l'authentification utilisateur via SAML.

Les étapes suivantes vous expliquent comment activer le provisionnement automatique des utilisateurs depuis IAM Identity Center PingOne à l'aide du protocole SCIM.

> **Note**
>
> Avant de commencer à déployer SCIM, nous vous recommandons de consulter d'abord leConsidérations relatives à l'utilisation du provisionnement automatique. Passez ensuite en revue les autres considérations dans la section suivante.

Rubriques

- Étape 2 : configurer le provisionnement dans PingOne
- (Facultatif) Étape 3 : Configuration des attributs utilisateur PingOne pour le contrôle d'accès dans IAM Identity Center
- (Facultatif) Transmission d'attributs pour le contrôle d'accès

Prérequis

Vous aurez besoin des éléments suivants avant de pouvoir commencer :

- Un PingOne abonnement ou un essai gratuit, avec des fonctionnalités d'authentification fédérée et de provisionnement. Pour plus d'informations sur la façon d'obtenir un essai gratuit, consultez le Ping Identitysite Web.
- Un compte compatible avec IAM Identity Center (gratuit). Pour plus d'informations, consultez la section Activer le centre d'identité IAM.
- L'application PingOne IAM Identity Center a été ajoutée à votre portail PingOne d'administration. Vous pouvez obtenir l'application PingOne IAM Identity Center à partir du catalogue PingOne d'applications. Pour des informations générales, voir Ajouter une application depuis le catalogue d'applications sur le Ping Identity site Web.
- Une connexion SAML entre votre PingOne instance et IAM Identity Center. Une fois que l'application PingOne IAM Identity Center a été ajoutée à votre portail PingOne d'administration, vous devez l'utiliser pour configurer une connexion SAML entre votre PingOne instance et IAM Identity Center. Utilisez les fonctionnalités de « téléchargement » et d' « importation » des métadonnées situées aux deux extrémités pour échanger des métadonnées SAML entre IAM Identity PingOne Center et IAM. Pour obtenir des instructions sur la configuration de cette connexion, consultez la PingOne documentation.

Considérations supplémentaires

Les considérations suivantes sont importantes et peuvent avoir une incidence sur PingOne la manière dont vous implémentez le provisionnement avec IAM Identity Center.

- Depuis octobre 2020, PingOne ne prend pas en charge le provisionnement de groupes via SCIM. Contactez-nous Ping pour obtenir les dernières informations sur le soutien aux groupes dans SCIM forPingOne.
- Les utilisateurs peuvent continuer à être approvisionnés PingOne après avoir désactivé le provisionnement dans le PingOne portail d'administration. Si vous devez mettre fin au

provisionnement immédiatement, supprimez le jeton porteur SCIM correspondant et/ou désactivez-le Approvisionnement automatique dans IAM Identity Center.

- Si un attribut d'un utilisateur est supprimé du magasin de données configuré dansPingOne, cet attribut ne sera pas supprimé de l'utilisateur correspondant dans IAM Identity Center. Il s'agit d'une limitation connue dans la mise en PingOne's œuvre du fournisseur. Si un attribut est modifié, le changement sera synchronisé avec IAM Identity Center.
- Voici quelques remarques importantes concernant votre configuration SAML dans PingOne :
  - IAM Identity Center ne prend en charge `emailaddress` que le `NameId` format. Cela signifie que vous devez choisir un attribut utilisateur unique dans votre répertoirePingOne, non nul et formaté sous forme d'e-mail/UPN (par exemple, user@domain.com) pour votre mappage SAML_SUBJECT dans. PingOne Email (Work) est une valeur raisonnable à utiliser pour tester les configurations avec le répertoire PingOne intégré.
  - Les utilisateurs qui se connectent PingOne avec une adresse e-mail contenant un caractère + peuvent ne pas être en mesure de se connecter à IAM Identity Center en raison d'erreurs telles que `'SAML_215'` ou`'Invalid input'`. Pour résoudre ce problèmePingOne, choisissez l'option Advanced pour le mappage SAML_SUBJECT dans les mappages d'attributs. Définissez ensuite le format Name ID à envoyer à SP : to urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddressdans le menu déroulant.

Étape 1 : activer le provisionnement dans IAM Identity Center

Dans cette première étape, vous utilisez la console IAM Identity Center pour activer le provisionnement automatique.

Pour activer le provisionnement automatique dans IAM Identity Center

1. Une fois que vous avez rempli les conditions requises, ouvrez la console IAM Identity Center.
2. Choisissez Paramètres dans le volet de navigation de gauche.
3. Sur la page Paramètres, recherchez la zone Informations de provisionnement automatique, puis choisissez Activer. Cela active immédiatement le provisionnement automatique dans IAM Identity Center et affiche les informations nécessaires sur le point de terminaison SCIM et le jeton d'accès.
4. Dans la boîte de dialogue de provisionnement automatique entrant, copiez chacune des valeurs des options suivantes. Vous devrez les coller ultérieurement lorsque vous configurerez le provisionnement dans votre IdP.

a. Point de terminaison SCIM

b. Jeton d'accès

5. Choisissez Fermer.

Maintenant que vous avez configuré le provisionnement dans la console IAM Identity Center, vous devez effectuer les tâches restantes à l'aide de l'application PingOne IAM Identity Center. Ces étapes sont décrites dans la procédure suivante.

Étape 2 : configurer le provisionnement dans PingOne

Utilisez la procédure suivante dans l'application PingOne IAM Identity Center pour activer le provisionnement avec IAM Identity Center. Cette procédure suppose que vous avez déjà ajouté l'application PingOne IAM Identity Center à votre portail PingOne d'administration. Si vous ne l'avez pas encore fait, reportez-vous à cette procédurePrérequis, puis exécutez-la pour configurer le provisionnement SCIM.

Pour configurer le provisionnement dans PingOne

1. Ouvrez l'application PingOne IAM Identity Center que vous avez installée dans le cadre de la configuration de SAML pour PingOne (Applications > Mes applications). veuillez consulter Prérequis.
2. Faites défiler la page vers le bas. Sous Configuration utilisateur, choisissez le lien complet pour accéder à la configuration de configuration de configuration utilisateur de votre connexion.
3. Sur la page Instructions de provisionnement, choisissez Passer à l'étape suivante.
4. Dans la procédure précédente, vous avez copié la valeur du point de terminaison SCIM dans IAM Identity Center. Collez cette valeur dans le champ URL SCIM de l'application PingOne IAM Identity Center. Assurez-vous de supprimer la barre oblique à la fin de l'URL. Dans la procédure précédente, vous avez également copié la valeur du jeton d'accès dans IAM Identity Center. Collez cette valeur dans le champ ACCESS_TOKEN de l'application PingOne IAM Identity Center.
5. Pour REMOVE_ACTION, choisissez Désactivé ou Supprimé (voir le texte de description sur la page pour plus de détails).
6. Sur la page Mappage des attributs, choisissez une valeur à utiliser pour l'assertion SAML_SUBJECT (`NameId`), en suivant les instructions données Considérations supplémentaires plus haut sur cette page. Choisissez ensuite Passer à l'étape suivante.

7. Sur la page Personnalisation des PingOne applications - IAM Identity Center, apportez les modifications de personnalisation souhaitées (facultatif), puis cliquez sur Passer à l'étape suivante.
8. Sur la page Accès aux groupes, choisissez les groupes contenant les utilisateurs que vous souhaitez activer pour le provisionnement et l'authentification unique à IAM Identity Center. Choisissez Passer à l'étape suivante.
9. Faites défiler la page vers le bas et choisissez Terminer pour commencer le provisionnement.
10. Pour vérifier que les utilisateurs ont été correctement synchronisés avec IAM Identity Center, revenez à la console IAM Identity Center et sélectionnez Utilisateurs. Les utilisateurs synchronisés depuis PingOne apparaîtront sur la page Utilisateurs. Ces utilisateurs peuvent désormais être affectés à des comptes et à des applications au sein d'IAM Identity Center.

    N'oubliez pas que PingOne cela ne prend pas en charge le provisionnement de groupes ou d'adhésions à des groupes via SCIM. Contactez-nous Ping pour plus d'informations.

(Facultatif) Étape 3 : Configuration des attributs utilisateur PingOne pour le contrôle d'accès dans IAM Identity Center

Il s'agit d'une procédure facultative PingOne si vous choisissez de configurer des attributs pour IAM Identity Center afin de gérer l'accès à vos AWS ressources. Les attributs que vous définissez PingOne sont transmis dans une assertion SAML à IAM Identity Center. Vous créez ensuite un ensemble d'autorisations dans IAM Identity Center pour gérer l'accès en fonction des attributs que vous avez transmisPingOne.

Avant de commencer cette procédure, vous devez d'abord activer la Attributs pour le contrôle d'accès fonctionnalité. Pour plus d'informations sur cette étape, consultez Activer et configurer les attributs pour le contrôle d'accès.

Pour configurer les attributs utilisateur PingOne pour le contrôle d'accès dans IAM Identity Center

1. Ouvrez l'application PingOne IAM Identity Center que vous avez installée dans le cadre de la configuration de SAML pour PingOne (Applications > Mes applications).
2. Choisissez Modifier, puis passez à l'étape suivante jusqu'à ce que vous arriviez à la page Mappages d'attributs.
3. Sur la page Mappages d'attributs, choisissez Ajouter un nouvel attribut, puis procédez comme suit. Vous devez effectuer ces étapes pour chaque attribut que vous ajouterez pour être utilisé dans IAM Identity Center à des fins de contrôle d'accès.

a. Dans le champ Attribut de l'application, entrez`https://aws.amazon.com/SAML/Attributes/AccessControl:`*`AttributeName`*. *`AttributeName`*Remplacez-le par le nom de l'attribut que vous attendez dans IAM Identity Center. Par exemple, `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Email`**.

b. Dans le champ Attribut ou valeur littérale d'Identity Bridge, sélectionnez les attributs utilisateur PingOne dans votre annuaire. Par exemple, Email (Work).

4. Cliquez sur Suivant à quelques reprises, puis sur Terminer.

(Facultatif) Transmission d'attributs pour le contrôle d'accès

Vous pouvez éventuellement utiliser la Attributs pour le contrôle d'accès fonctionnalité d'IAM Identity Center pour transmettre un `Attribute` élément dont l'`Name`attribut est défini sur. `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`** Cet élément vous permet de transmettre des attributs en tant que balises de session dans l'assertion SAML. Pour plus d'informations sur les balises de session, consultez la section Transmission de balises de session AWS STS dans le guide de l'utilisateur IAM.

Pour transmettre des attributs en tant que balises de session, incluez l'élément `AttributeValue` qui spécifie la valeur de la balise. Par exemple, pour transmettre la paire clé-valeur du tag`CostCenter = blue`, utilisez l'attribut suivant.

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

Si vous devez ajouter plusieurs attributs, incluez un `Attribute` élément distinct pour chaque balise.

Démarrez avec les tâches courantes dans IAM Identity Center

Si vous êtes un nouvel utilisateur d'IAM Identity Center, le flux de travail de base pour commencer à utiliser le service est le suivant :

1. Connectez-vous à la console de votre compte de gestion si vous utilisez une instance organisationnelle d'IAM Identity Center ou Compte AWS si vous utilisez une instance de compte d'IAM Identity Center et accédez à la console IAM Identity Center.
2. Sélectionnez le répertoire que vous utilisez pour stocker les identités de vos utilisateurs et groupes à partir de la console IAM Identity Center. IAM Identity Center vous fournit un répertoire par défaut que vous pouvez utiliser pour configurer l'accès des utilisateurs. Si vous préférez utiliser une autre source d'identité, vous pouvez connecter votre Active Directory ou un fournisseur d'identité externe.
3. Pour les instances d'organisation, attribuez l'accès aux utilisateurs en Comptes AWS sélectionnant les comptes de votre organisation, puis en sélectionnant les utilisateurs ou les groupes dans votre annuaire et les autorisations que vous souhaitez leur accorder.
4. Donnez aux utilisateurs l'accès aux applications en :
   a. Configurez des applications SAML 2.0 gérées par le client en sélectionnant l'une des applications préintégrées dans le catalogue d'applications ou en ajoutant votre propre application SAML 2.0.
   b. Configurez les propriétés de l'application.
   c. Attribuez aux utilisateurs l'accès à l'application. Nous vous recommandons d'attribuer l'accès aux utilisateurs par le biais de l'appartenance à un groupe plutôt qu'en ajoutant des autorisations utilisateur individuelles. Avec les groupes, vous pouvez accorder ou refuser des autorisations à des groupes d'utilisateurs, au lieu d'appliquer ces autorisations à chaque individu. Si un utilisateur est transféré dans une autre organisation, il vous suffit de le déplacer vers un autre groupe. L'utilisateur reçoit alors automatiquement les autorisations nécessaires à la nouvelle organisation.
5. Si vous utilisez le répertoire IAM Identity Center par défaut, indiquez à vos utilisateurs comment se connecter au portail AWS d'accès. Les nouveaux utilisateurs d'IAM Identity Center doivent activer leurs informations d'identification avant de pouvoir les utiliser pour se connecter au portail AWS d'accès. Pour plus d'informations, voir Se connecter au portail AWS d'accès dans le guide de Connexion à AWS l'utilisateur

Les rubriques de cette section vous aident à vous familiariser avec les tâches courantes effectuées une fois que vous avez terminé la configuration initiale d'IAM Identity Center.

Si vous n'avez pas encore activé IAM Identity Center, consultezActivant AWS IAM Identity Center.

Rubriques

- Crée un jeu d'autorisations.
- Attribuer un Compte AWS accès à un utilisateur d'IAM Identity Center
- Connectez-vous au portail d' AWS accès à l'aide de vos identifiants IAM Identity Center
- Attribuer Compte AWS l'accès aux groupes
- Configurez l'accès par authentification unique à vos applications
- Afficher les attributions des utilisateurs et des groupes

Crée un jeu d'autorisations.

Les ensembles d'autorisations sont stockés dans IAM Identity Center et définissent le niveau d'accès des utilisateurs et des groupes à un Compte AWS. Le premier ensemble d'autorisations que vous créez est le jeu d'autorisations administratives. Si vous avez terminé l'un d'entre eux, Tutoriels de mise en route vous avez déjà créé votre ensemble d'autorisations administratives. Utilisez cette procédure pour créer des ensembles d'autorisations, comme décrit dans la rubrique Politiques AWS gérées pour les fonctions professionnelles du Guide de l'utilisateur IAM.

1. Procédez de l'une des manières suivantes pour vous connecter au AWS Management Console.

   - Nouvel utilisateur AWS (utilisateur root) : connectez-vous en tant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.
   - Vous utilisez déjà AWS (informations d'identification IAM) : connectez-vous à l'aide de vos informations d'identification IAM avec des autorisations administratives.
2. Ouvrez la console IAM Identity Center.
3. Dans le volet de navigation d'IAM Identity Center, sous Autorisations multi-comptes, sélectionnez Ensembles d'autorisations.
4. Choisissez Create permission set (Créer un jeu d'autorisations).

   a. Sur la page Sélectionner le type d'ensemble d'autorisations, dans la section Type d'ensemble d'autorisations, choisissez Ensemble d'autorisations prédéfini.

b. Dans la section Politique pour un ensemble d'autorisations prédéfini, choisissez l'une des options suivantes :

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

5. Sur la page Spécifier les détails de l'ensemble d'autorisations, conservez les paramètres par défaut et choisissez Next. Le paramètre par défaut limite votre session à une heure.
6. Sur la page Réviser et créer, confirmez les points suivants :

1. Pour l'étape 1 : Sélectionnez le type d'ensemble d'autorisations, affiche le type d'ensemble d'autorisations que vous avez choisi.
2. Pour l'étape 2 : définir les détails de l'ensemble d'autorisations, affiche le nom du jeu d'autorisations que vous avez choisi.
3. Choisissez Créer.

Créez un ensemble d'autorisations qui applique les autorisations du moindre privilège

Pour suivre la meilleure pratique consistant à appliquer des autorisations de moindre privilège, après avoir créé un ensemble d'autorisations administratives, vous créez un ensemble d'autorisations plus restrictif et vous l'attribuez à un ou plusieurs utilisateurs. Les ensembles d'autorisations créés lors de la procédure précédente constituent un point de départ pour évaluer le niveau d'accès aux ressources dont vos utilisateurs ont besoin. Pour passer aux autorisations du moindre privilège, vous pouvez exécuter IAM Access Analyzer pour surveiller les principaux à l'aide AWS de politiques gérées. Après avoir appris quelles autorisations ils utilisent, vous pouvez rédiger une politique

personnalisée ou générer une politique avec uniquement les autorisations requises pour votre équipe.

Avec IAM Identity Center, vous pouvez attribuer plusieurs ensembles d'autorisations au même utilisateur. Votre utilisateur administratif doit également se voir attribuer des ensembles d'autorisations supplémentaires, plus restrictifs. De cette façon, ils peuvent accéder à vous uniquement Compte AWS avec les autorisations requises, au lieu de toujours utiliser leurs autorisations administratives.

Par exemple, si vous êtes développeur, après avoir créé votre utilisateur administratif dans IAM Identity Center, vous pouvez créer un nouvel ensemble d'autorisations qui octroie des `PowerUserAccess` autorisations, puis vous attribuer cet ensemble d'autorisations. Contrairement à l'ensemble d'autorisations administratives, qui utilise des `AdministratorAccess` autorisations, le jeu `PowerUserAccess` d'autorisations ne permet pas la gestion des utilisateurs et des groupes IAM. Lorsque vous vous connectez au portail AWS d'accès pour accéder à votre AWS compte, vous pouvez choisir d'effectuer des tâches de développement dans le compte `PowerUserAccess` plutôt que de le `AdministratorAccess` faire.

Gardez les considérations suivantes à l'esprit :

- Pour commencer rapidement à créer un ensemble d'autorisations plus restrictif, utilisez un ensemble d'autorisations prédéfini plutôt qu'un ensemble d'autorisations personnalisé.

  Avec un ensemble d'autorisations prédéfini, qui utilise des autorisations prédéfinies, vous choisissez une seule politique AWS gérée parmi la liste des politiques disponibles. Chaque politique accorde un niveau spécifique d'accès aux AWS services et aux ressources ou des autorisations pour une fonction professionnelle commune. Pour plus d'informations sur chacune de ces politiques, consultez la section Politiques AWS gérées pour les fonctions de travail.
- Vous pouvez configurer la durée de session pour un ensemble d'autorisations afin de contrôler la durée pendant laquelle un utilisateur est connecté à un Compte AWS.

  Lorsque les utilisateurs se fédérent dans leur Compte AWS et utilisent la console de AWS gestion ou l'interface de ligne de AWS commande (AWS CLI), IAM Identity Center utilise le paramètre de durée de session figurant sur le jeu d'autorisations pour contrôler la durée de la session. Par défaut, la valeur de la durée de session, qui détermine la durée pendant laquelle un utilisateur peut être connecté ou Compte AWS avant AWS de le déconnecter de la session, est définie sur une heure. Vous pouvez spécifier une valeur maximale de 12 heures. Pour plus d'informations, consultez Définir la durée de la session.

- Vous pouvez également configurer la durée de session du portail d' AWS accès pour contrôler la durée pendant laquelle un utilisateur du personnel est connecté au portail.

  Par défaut, la valeur de la durée maximale de session, qui détermine la durée pendant laquelle un utilisateur du personnel peut se connecter au portail d' AWS accès avant de devoir s'authentifier à nouveau, est de huit heures. Vous pouvez spécifier une valeur maximale de 90 jours. Pour plus d'informations, consultez Configurer la durée de session du portail d' AWS accès et des applications intégrées d'IAM Identity Center.
- Lorsque vous vous connectez au portail AWS d'accès, choisissez le rôle qui fournit les autorisations les moins privilégiées.

  Chaque ensemble d'autorisations que vous créez et attribuez à votre utilisateur apparaît comme un rôle disponible dans le portail AWS d'accès. Lorsque vous vous connectez au portail en tant qu'utilisateur, choisissez le rôle qui correspond à l'ensemble d'autorisations le plus restrictif que vous pouvez utiliser pour effectuer des tâches dans le compte, plutôt que`AdministratorAccess`.
- Vous pouvez ajouter d'autres utilisateurs à IAM Identity Center et leur attribuer des ensembles d'autorisations existants ou nouveaux.

  Pour plus d'informations, voir,Attribuer Compte AWS l'accès aux groupes.

Attribuer un Compte AWS accès à un utilisateur d'IAM Identity Center

Pour configurer Compte AWS l'accès d'un utilisateur du centre d'identité IAM, vous devez attribuer à l'utilisateur l'ensemble d'autorisations Compte AWS et.

1. Procédez de l'une des manières suivantes pour vous connecter au AWS Management Console.
   - Nouvel utilisateur AWS (utilisateur root) : connectez-vous en tant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.
   - Vous utilisez déjà AWS (informations d'identification IAM) : connectez-vous à l'aide de vos informations d'identification IAM avec des autorisations administratives.
2. Ouvrez la console IAM Identity Center.
3. Dans le volet de navigation, sous Autorisations multi-comptes, sélectionnez Comptes AWS.

4. Sur la Comptes AWSpage, une liste arborescente de votre organisation s'affiche. Cochez la case à côté de Compte AWS laquelle vous souhaitez attribuer l'accès. Si vous configurez l'accès administratif pour IAM Identity Center, cochez la case à côté du compte de gestion.
5. Choisissez Attribuer des utilisateurs ou des groupes.
6. Pour l'étape 1 : sélectionner les utilisateurs et les groupes, sur la page Attribuer des utilisateurs et des groupes au « ***Compte AWS nom*** », procédez comme suit :

   1. Dans l'onglet Utilisateurs, sélectionnez l'utilisateur auquel vous souhaitez accorder des autorisations administratives.

      Pour filtrer les résultats, commencez à saisir le nom de l'utilisateur souhaité dans le champ de recherche.
   2. Après avoir confirmé que le bon utilisateur est sélectionné, choisissez Next.
7. Pour l'étape 2 : sélectionner des ensembles d'autorisations, sur la page Attribuer des ensembles d'autorisations à « ***Compte AWS nommer*** », sous Ensembles d'autorisations, sélectionnez un ensemble d'autorisations pour définir le niveau d'accès dont disposent les utilisateurs et les groupes à cet égard Compte AWS.
8. Choisissez Suivant.
9. Pour l'étape 3 : Réviser et envoyer, sur la page Réviser et envoyer les devoirs au « ***Compte AWS nom*** », procédez comme suit :

   1. Vérifiez l'utilisateur et l'ensemble d'autorisations sélectionnés.
   2. Après avoir confirmé que l'ensemble d'autorisations est attribué au bon utilisateur, choisissez Soumettre.

   > **Important**
   >
   > Le processus d'attribution des utilisateurs peut prendre quelques minutes. Laissez cette page ouverte jusqu'à ce que le processus soit terminé avec succès.
10. Si l'une des conditions suivantes s'applique, suivez les étapes décrites Inviter les utilisateurs à utiliser le MFA pour activer le MFA pour IAM Identity Center :

    - Vous utilisez le répertoire Identity Center par défaut comme source d'identité.
    - Vous utilisez un AWS Managed Microsoft AD annuaire ou un répertoire autogéré dans Active Directory comme source d'identité et vous n'utilisez pas RADIUS AWS Directory Service MFA avec.

> **Note**
>
> Si vous utilisez un fournisseur d'identité externe, notez que c'est l'IdP externe, et non IAM Identity Center, qui gère les paramètres MFA. L'authentification MFA dans IAM Identity Center n'est pas prise en charge pour une utilisation par des tiers. IdPs

Lorsque vous configurez l'accès au compte pour l'utilisateur administratif, IAM Identity Center crée un rôle IAM correspondant. Ce rôle, qui est contrôlé par IAM Identity Center, est créé dans le répertoire approprié Compte AWS, et les politiques spécifiées dans le jeu d'autorisations sont associées au rôle.

Connectez-vous au portail d' AWS accès à l'aide de vos identifiants IAM Identity Center

Le portail AWS d'accès fournit aux utilisateurs d'IAM Identity Center un accès par authentification unique à toutes les applications Comptes AWS et applications qui leur sont assignées via un portail Web.

Procédez comme suit pour confirmer que l'utilisateur d'IAM Identity Center peut se connecter au portail AWS d'accès et accéder au Compte AWS.

1. Procédez de l'une des manières suivantes pour vous connecter au AWS Management Console.
   - Nouvel utilisateur AWS (utilisateur root) : connectez-vous en tant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.
   - Vous utilisez déjà AWS (informations d'identification IAM) : connectez-vous à l'aide de vos informations d'identification IAM et sélectionnez un rôle d'administrateur.
2. Ouvrez la console IAM Identity Center.
3. Dans le panneau de navigation, sélectionnez Dashboard (Tableau de bord).
4. Sur la page Tableau de bord, sous Résumé des paramètres, choisissez l'URL du portail AWS d'accès.
5. Connectez-vous en utilisant l'une des méthodes suivantes :

- Si vous utilisez Active Directory ou un fournisseur d'identité externe (IdP) comme source d'identité, connectez-vous à l'aide des informations d'identification de l'utilisateur Active Directory ou IdP.
- Si vous utilisez le répertoire Identity Center par défaut comme source d'identité, connectez-vous en utilisant le nom d'utilisateur que vous avez spécifié lors de la création de l'utilisateur et le nouveau mot de passe que vous avez spécifié pour l'utilisateur.

1. Dans l'onglet Comptes, localisez-le Compte AWS et développez-le.
2. Les rôles disponibles s'affichent. Par exemple, si l'ensemble d'autorisations et les AdministratorAccessensembles d'autorisations de facturation vous sont attribués, ces rôles sont affichés dans le portail AWS d'accès. Choisissez le nom du rôle IAM que vous souhaitez utiliser pour la session.
3. Si vous êtes redirigé vers la console AWS de gestion, vous avez correctement configuré l'accès au Compte AWS.

> **Note**
>
> Si aucune autorisation n'est Comptes AWSrépertoriée, il est probable que l'utilisateur n'ait pas encore reçu d'ensemble d'autorisations pour ce compte. Pour obtenir des instructions sur l'attribution d'utilisateurs à un ensemble d'autorisations, consultezAttribuer un accès utilisateur à Comptes AWS.

Maintenant que vous avez confirmé que vous pouvez vous connecter à l'aide des informations d'identification IAM Identity Center, passez au navigateur que vous avez utilisé pour vous connecter AWS Management Console et déconnectez-vous à partir de vos informations d'identification d'utilisateur root ou d'utilisateur IAM.

> **Important**
>
> Nous vous recommandons vivement d'utiliser les informations d'identification de l'utilisateur administratif d'IAM Identity Center lorsque vous vous connectez au portail d' AWS accès pour effectuer des tâches administratives au lieu d'utiliser les informations d'identification de l'utilisateur IAM ou de l'utilisateur root. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour permettre à d'autres utilisateurs d'accéder à vos comptes et applications, et pour administrer

IAM Identity Center, créez et attribuez des ensembles d'autorisations uniquement via IAM Identity Center.

Attribuer Compte AWS l'accès aux groupes

Après avoir créé un utilisateur administratif dans IAM Identity Center et créé des ensembles d'autorisations supplémentaires que vous pouvez utiliser pour effectuer des tâches avec les autorisations les moins privilégiées, vous pouvez donner accès Comptes AWS à vos deux groupes d'utilisateurs.

Nous vous recommandons d'attribuer l'accès directement à des groupes plutôt qu'à des utilisateurs individuels. Par exemple, si vous créez des groupes et des ensembles d'autorisations basés sur des unités organisationnelles, si un utilisateur passe à une autre unité organisationnelle, vous déplacez simplement cet utilisateur vers un autre groupe et il reçoit automatiquement les autorisations nécessaires pour la nouvelle unité organisationnelle et perd les autorisations de l'unité organisationnelle précédente.

Pour attribuer un accès à un groupe d'utilisateurs à Comptes AWS

1. Ouvrez la console IAM Identity Center.

   > **Note**
   >
   > Si votre source d'identité est, AWS Managed Microsoft AD assurez-vous que la console IAM Identity Center utilise la région dans laquelle se trouve votre AWS Managed Microsoft AD répertoire avant de passer à l'étape suivante.

2. Dans le volet de navigation, sous Autorisations multi-comptes, sélectionnez Comptes AWS.
3. Sur la Comptes AWSpage, une liste arborescente de votre organisation apparaît. Cochez la case à côté d'une ou de plusieurs Comptes AWS personnes auxquelles vous souhaitez attribuer un accès par authentification unique.

   > **Note**
   >
   > Vous pouvez en sélectionner jusqu'à 10 Comptes AWS par ensemble d'autorisations.

4. Choisissez Attribuer des utilisateurs ou des groupes.

5. Pour l'étape 1 : Sélectionnez les utilisateurs et les groupes, sur la page Affecter des utilisateurs et des groupes à « ***AWS-account-name*** », sélectionnez l'onglet Groupes, puis choisissez un ou plusieurs groupes.

   Pour filtrer les résultats, commencez à taper le nom du groupe souhaité dans le champ de recherche.

   Pour afficher les groupes que vous avez sélectionnés, choisissez le triangle latéral à côté de Utilisateurs et groupes sélectionnés.

   Après avoir confirmé que les bons groupes sont sélectionnés, choisissez Next.

6. Pour l'étape 2 : Sélection des ensembles d'autorisations, sur la page Attribuer des ensembles d'autorisations à « ***AWS-account-name*** », sélectionnez un ou plusieurs ensembles d'autorisations

   > **Note**
   >
   > Si vous n'avez pas créé l'ensemble d'autorisations souhaité avant de commencer cette procédure, choisissez Créer un ensemble d'autorisations et suivez les étapes décrites dansCrée un jeu d'autorisations.. Après avoir créé les ensembles d'autorisations que vous souhaitez appliquer, dans la console IAM Identity Center, revenez Comptes AWSet suivez les instructions jusqu'à ce que vous atteigniez l'étape 2 : Sélectionnez les ensembles d'autorisations. Lorsque vous atteignez cette étape, sélectionnez les nouveaux ensembles d'autorisations que vous avez créés et passez à l'étape suivante de cette procédure.

   Après avoir confirmé que les ensembles d'autorisations appropriés sont sélectionnés, choisissez Next.

7. Pour l'étape 3 : Révision et envoi, sur la page Réviser et envoyer les assignations à « ***AWS-account-name*** », procédez comme suit :

   1. Passez en revue les groupes sélectionnés et les ensembles d'autorisations.
   2. Après avoir confirmé que les groupes et ensembles d'autorisations appropriés sont sélectionnés, choisissez Soumettre.

> **Important**
>
> Le processus d'attribution de groupe peut prendre quelques minutes. Laissez cette page ouverte jusqu'à ce que le processus soit terminé avec succès.

> **Note**
>
> Vous devrez peut-être accorder à des utilisateurs ou à des groupes des autorisations pour opérer dans le compte AWS Organizations de gestion. Comme il s'agit d'un compte à privilèges élevés, des restrictions de sécurité supplémentaires nécessitent que vous disposiez de la FullAccess politique IAM ou d'autorisations équivalentes avant de pouvoir le configurer. Ces restrictions de sécurité supplémentaires ne sont requises pour aucun des comptes membres de votre AWS organisation.

Vous pouvez également utiliser AWS CloudFormationpour créer et attribuer des ensembles d'autorisations et affecter des utilisateurs à ces ensembles d'autorisations. Les utilisateurs peuvent ensuite se connecter au portail AWS d'accès ou utiliser les commandes AWS Command Line Interface (AWS CLI).

Configurez l'accès par authentification unique à vos applications

IAM Identity Center prend en charge deux types d'applications : les applications AWS gérées et les applications gérées par le client.

AWS les applications gérées sont configurées directement depuis les consoles d'application pertinentes ou via les API de l'application.

Les applications gérées par le client doivent être ajoutées à la console IAM Identity Center et configurées avec les métadonnées appropriées à la fois pour IAM Identity Center et pour le fournisseur de services. Vous pouvez choisir parmi un catalogue d'applications couramment utilisées qui prennent en charge le protocole SAML 2.0, ou vous pouvez configurer vos propres applications SAML 2.0 ou les applications OAuth 2.0.

Les étapes de configuration pour configurer l'accès par authentification unique aux applications varient en fonction du type d'application.

Configuration d'une application AWS gérée

AWS les applications gérées telles qu'Amazon Managed Grafana et Amazon Monitron s'intègrent à IAM Identity Center et peuvent l'utiliser pour l'authentification et les services d'annuaire. Pour configurer une application AWS gérée afin qu'elle fonctionne avec IAM Identity Center, vous devez configurer l'application directement depuis la console du service applicable, ou vous devez utiliser les API de l'application.

Configuration d'une application à partir du catalogue d'applications

Vous pouvez sélectionner une application SAML 2.0 dans un catalogue d'applications couramment utilisées dans la console IAM Identity Center. Utilisez cette procédure pour configurer une relation de confiance SAML 2.0 entre IAM Identity Center et le fournisseur de services de votre application.

Pour configurer une application à partir du catalogue d'applications

1. Ouvrez la console IAM Identity Center.
2. Choisissez Applications.
3. Choisissez l'onglet Géré par le client.
4. Choisissez Add application (Ajouter une application).
5. Sur la page Sélectionner le type d'application, sous Préférences de configuration, choisissez Je souhaite sélectionner une application dans le catalogue.
6. Sous Catalogue d'applications, commencez à taper le nom de l'application que vous souhaitez ajouter dans le champ de recherche.
7. Choisissez le nom de l'application dans la liste lorsqu'elle apparaît dans les résultats de recherche, puis cliquez sur Suivant.
8. Sur la page Configurer l'application, les champs Nom d'affichage et Description sont préremplis avec les informations pertinentes pour l'application. Vous pouvez modifier ces informations.
9. Sous les métadonnées du IAM Identity Center, procédez comme suit :

    a. Dans le fichier de métadonnées SAML d'IAM Identity Center, choisissez Télécharger pour télécharger les métadonnées du fournisseur d'identité.

    b. Sous le certificat IAM Identity Center, choisissez Télécharger le certificat pour télécharger le certificat du fournisseur d'identité.

> **Note**
>
> Vous aurez besoin de ces fichiers ultérieurement lorsque vous configurerez l'application à partir du site Web du fournisseur de services. Suivez les instructions de ce fournisseur.

10. (Facultatif) Sous Propriétés de l'application, vous pouvez spécifier l'URL de démarrage de l'application, l'état du relais et la durée de la session. Pour plus d'informations, consultez Configuration des propriétés de l'application dans la console IAM Identity Center.
11. Sous Métadonnées de l'application, effectuez l'une des opérations suivantes :
    a. Si vous avez un fichier de métadonnées, choisissez Télécharger le fichier de métadonnées SAML de l'application. Sélectionnez ensuite Choisir un fichier pour rechercher et sélectionner le fichier de métadonnées.
    b. Si vous n'avez pas de fichier de métadonnées, choisissez Tapez manuellement vos valeurs de métadonnées, puis fournissez l'URL de l'application ACS et les valeurs d'audience SAML de l'application.
12. Sélectionnez Envoyer. Vous êtes redirigé vers la page de détails de l'application que vous venez d'ajouter.

Configurez votre propre application SAML 2.0

Utilisez cette procédure pour configurer votre propre relation de confiance SAML 2.0 entre IAM Identity Center et le fournisseur de services de votre propre application SAML 2.0. Avant de commencer cette procédure, vérifiez que vous avez le certificat et les fichiers d'échange de métadonnées du fournisseur de services afin de finaliser la configuration de l'approbation.

Pour configurer votre propre application SAML 2.0

1. Ouvrez la console IAM Identity Center.
2. Choisissez Applications.
3. Choisissez l'onglet Géré par le client.
4. Choisissez Add application (Ajouter une application).
5. Sur la page Sélectionner le type d'application, sous Préférences de configuration, choisissez J'ai une application que je souhaite configurer.
6. Sous Type d'application, choisissez SAML 2.0.

7. Choisissez Suivant.
8. Sur la page Configurer l'application, sous Configurer l'application, entrez un nom d'affichage pour l'application, tel que**MyApp**. Entrez ensuite une description.
9. Sous les métadonnées du IAM Identity Center, procédez comme suit :

    a. Dans le fichier de métadonnées SAML d'IAM Identity Center, choisissez Télécharger pour télécharger les métadonnées du fournisseur d'identité.

    b. Sous le certificat IAM Identity Center, choisissez Télécharger pour télécharger le certificat du fournisseur d'identité.

    > **Note**
    >
    > Vous aurez besoin de ces fichiers par la suite pour configurer l'application personnalisée sur le site web du fournisseur de services.

10. (Facultatif) Sous Propriétés de l'application, vous pouvez également spécifier l'URL de démarrage de l'application, l'état du relais et la durée de la session. Pour plus d'informations, consultez Configuration des propriétés de l'application dans la console IAM Identity Center.
11. Sous Métadonnées de l'application, choisissez Tapez manuellement vos valeurs de métadonnées. Indiquez ensuite l'URL ACS de l'application et les valeurs d'audience SAML de l'application.
12. Sélectionnez Envoyer. Vous êtes redirigé vers la page de détails de l'application que vous venez d'ajouter.

Une fois que vous avez configuré vos applications, vos utilisateurs peuvent y accéder depuis leur portail AWS d'accès en fonction des autorisations que vous leur avez attribuées.

Si vous avez des applications gérées par le client qui prennent en charge OAuth 2.0 et que vos utilisateurs ont besoin d'accéder à des AWS services depuis ces applications, vous pouvez utiliser la propagation d'identité sécurisée. Grâce à la propagation sécurisée des identités, un utilisateur peut se connecter à une application, et cette application peut transmettre l'identité de l'utilisateur dans les demandes d'accès aux données AWS des services. Pour plus d'informations, consultez Utilisation d'une propagation d'identité fiable avec des applications gérées par le client.

Pour obtenir plus d'informations sur les types d'application pris en charge, consultez Gérez l'accès aux applications.

Afficher les attributions des utilisateurs et des groupes

Vous pouvez voir qui a accès à quoi dans IAM Identity Center sur les pages Utilisateurs et Groupes. Utilisez cette procédure pour afficher le niveau d'accès des utilisateurs aux AWS comptes, aux ensembles d'autorisations, aux applications et aux groupes.

1. Ouvrez la console IAM Identity Center.
2. Choisissez Utilisateurs ou Groupes selon que vous souhaitez modifier un groupe d'utilisateurs ou un utilisateur attribué individuellement.
3. Choisissez un utilisateur ou un groupe dans la liste.
4. Choisissez si vous souhaitez afficher les attributions de compte, les attributions de candidature ou les affectations de groupe :

   - AWS attributions de comptes et d'ensembles d'autorisations
     1. Sélectionnez l'onglet Accounts.
     2. Sélectionnez un compte dans la liste pour afficher les attributions des ensembles d'autorisations aux utilisateurs et aux groupes.
     3. Sélectionnez un ensemble d'autorisations à consulter pour consulter les détails de la politique et des attributions.
   - Attributions de candidatures
     1. Choisissez l'onglet Applications pour voir quelles applications sont attribuées à un utilisateur ou à un groupe.
     2. Sélectionnez une application dans la liste pour afficher les détails de l'affectation.
   - Missions de groupe
     1. Sur la page Utilisateurs, choisissez l'onglet Groupes.
     2. Sélectionnez un groupe pour afficher les attributions de groupe attribuées à un utilisateur.

Gérer les instances d'organisation et de compte d'IAM Identity Center

Une instance est un déploiement unique d'IAM Identity Center. Deux types d'instances sont disponibles pour IAM Identity Center : les instances d'organisation et les instances de compte.

Compte AWS types pouvant activer IAM Identity Center

Pour activer IAM Identity Center, connectez-vous au en AWS Management Console utilisant l'une des informations d'identification suivantes, selon le type d'instance que vous souhaitez créer :

- Votre compte AWS Organizations de gestion (recommandé) : obligatoire pour créer une instance organisationnelle d'IAM Identity Center. Utilisez une instance d'organisation pour les autorisations multi-comptes et les attributions d'applications au sein de l'organisation.
- Votre compte de AWS Organizations membre : à utiliser pour créer une instance de compte d'IAM Identity Center afin de permettre l'attribution d'applications au sein de ce compte membre. Un ou plusieurs comptes dotés d'une instance de niveau membre peuvent exister dans une organisation.
- Une instance autonome Compte AWS : à utiliser pour créer une instance d'organisation ou une instance de compte d'IAM Identity Center. Le système autonome Compte AWS n'est pas géré par AWS Organizations. Une seule instance d'IAM Identity Center peut être associée à une instance autonome Compte AWS et vous pouvez utiliser l'instance pour les attributions d'applications au sein de cette instance autonome. Compte AWS

Capacité	Instance dans le compte AWS Organizations de gestion (recommandé)	Instance dans un compte membre	Instance dans un environnement autonome Compte AWS
Gestion des utilisateurs	 Oui	 Oui	 Oui

Capacité	Instance dans le compte AWS Organizations de gestion (recommandé)	Instance dans un compte membre	Instance dans un environnement autonome Compte AWS
AWS portail d'accès pour un accès par authentification unique à vos applications AWS gérées	 Oui	 Oui	 Oui
Applications gérées par le client OAuth 2.0 (OIDC)	 Oui	 Oui	 Oui
Autorisations multi-comptes	 Oui	 Non	 Non
AWS portail d'accès pour un accès par authentification unique à votre Comptes AWS	 Oui	 Non	 Non
Applications SAML 2.0 gérées par le client	 Oui	 Non	 Non
L'administrateur délégué peut gérer l'instance	 Oui	 Non	 Non

Rubriques

- Instances organisationnelles d'IAM Identity Center

- Instances de compte d'IAM Identity Center
- Activer les instances de compte dans la console IAM Identity Center
- Contrôlez la création d'instances de compte avec les politiques de contrôle des services
- Création d'une instance de compte d'IAM Identity Center

Instances organisationnelles d'IAM Identity Center

Lorsque vous activez IAM Identity Center conjointement avec AWS Organizations, vous créez une instance organisationnelle d'IAM Identity Center. Votre instance d'organisation doit être activée dans votre compte de gestion et vous pouvez gérer de manière centralisée l'accès des utilisateurs et des groupes avec une seule instance d'organisation. Vous ne pouvez avoir qu'une seule instance d'organisation pour chaque compte de gestion dans AWS Organizations.

Si vous avez activé IAM Identity Center avant le 15 novembre 2023, vous disposez d'une instance organisationnelle d'IAM Identity Center.

Quand utiliser une instance d'organisation

Une instance d'organisation est la principale méthode d'activation d'IAM Identity Center et, dans la plupart des cas, une instance d'organisation est recommandée. Les instances d'organisation offrent les avantages suivants :

- Support pour toutes les fonctionnalités d'IAM Identity Center, y compris la gestion des autorisations pour plusieurs Comptes AWS membres de votre organisation et l'attribution d'un accès aux applications gérées par les clients.
- Réduire le nombre de points de gestion : une instance d'organisation possède un point de gestion unique, le compte de gestion. Nous vous recommandons d'activer une instance d'organisation plutôt qu'une instance de compte afin de réduire le nombre de points de gestion.
- Contrôler la création d'instances de compte : vous pouvez contrôler si des instances de compte peuvent être créées par les comptes des membres de votre organisation tant que vous n'avez pas déployé d'instance d'IAM Identity Center dans votre organisation dans une région optionnelle (Région AWS qui est désactivée par défaut).

Instances de compte d'IAM Identity Center

Avec une instance de compte d'IAM Identity Center, vous pouvez déployer des applications AWS gérées prises en charge et des applications gérées par le client basées sur OIDC. Les instances de compte prennent en charge les déploiements isolés d'applications en une seule instance Compte AWS, en tirant parti des fonctionnalités du portail d'identité et d'accès du personnel d'IAM Identity Center.

Les instances de compte sont liées à une instance unique Compte AWS et sont utilisées uniquement pour gérer l'accès des utilisateurs et des groupes pour les applications prises en charge dans le même compte et Région AWS. Vous êtes limité à une instance de compte par Compte AWS. Vous pouvez créer une instance de compte à partir de l'une des méthodes suivantes :

- Un compte de membre dans AWS Organizations.
- Un appareil autonome Compte AWS qui n'est pas géré par AWS Organizations.

Contraintes de disponibilité pour les comptes membres

Vous pouvez déployer une instance de compte dans un compte membre d'une organisation si les conditions suivantes sont réunies :

- Aucune instance d'IAM Identity Center n'était déployée dans votre organisation avant le 15 novembre 2023.
- Vous avez déjà déployé une instance d'IAM Identity Center dans votre organisation avant le 15 novembre 2023, et votre administrateur a autorisé les comptes membres à créer des instances de compte d'IAM Identity Center.
- Votre administrateur n'a pas créé de politique de contrôle des services qui empêche les comptes membres de créer des instances de compte.
- Quoi qu'il en soit, vous n'avez pas encore d'instance d'IAM Identity Center dans ce même compte. Région AWS
- Vous travaillez dans un environnement Région AWS où IAM Identity Center n'est pas disponible. Pour plus d'informations sur les régions, consultezAWS IAM Identity Center Disponibilité de la région.

Rubriques

- Considérations relatives aux instances de compte
- AWS applications gérées prenant en charge les instances de compte

Quand utiliser les instances de compte

Dans la plupart des cas, une instance d'organisation est recommandée. Les instances de compte ne doivent être utilisées que si l'un des scénarios suivants s'applique :

- Vous souhaitez tester temporairement une application AWS gérée prise en charge afin de déterminer si l'application répond aux besoins de votre entreprise.
- Vous n'avez pas l'intention d'adopter IAM Identity Center au sein de votre organisation, mais vous souhaitez prendre en charge une ou plusieurs applications AWS gérées.
- Vous disposez d'une instance d'organisation d'IAM Identity Center, mais vous souhaitez déployer une application AWS gérée prise en charge vers un ensemble isolé d'utilisateurs distincts des utilisateurs de votre instance d'organisation.

> **Important**
>
> Si vous envisagez d'utiliser IAM Identity Center pour prendre en charge les applications de plusieurs comptes, créez une instance d'organisation et n'utilisez pas d'instances de compte.

Considérations relatives aux instances de compte

Une instance de compte est conçue pour des cas d'utilisation spécialisés et propose un sous-ensemble de fonctionnalités disponibles pour une instance d'organisation. Tenez compte des points suivants avant de créer une instance de compte :

- Les instances de compte ne prennent pas en charge les ensembles d'autorisations et ne prennent donc pas en charge l'accès à Comptes AWS.
- Vous ne pouvez pas convertir une instance de compte en instance d'organisation.
- Vous ne pouvez pas fusionner une instance de compte dans une instance d'organisation.
- Sélectionnez uniquement les instances de compte de AWS applications gérées support.
- Utilisez des instances de compte pour les utilisateurs isolés qui utiliseront les applications d'un seul compte et pendant toute la durée de vie des applications utilisées.

- Les applications associées à une instance de compte doivent rester attachées à l'instance de compte jusqu'à ce que vous supprimiez l'application et ses ressources.
- Une instance de compte doit rester Compte AWS là où elle a été créée.

AWS applications gérées prenant en charge les instances de compte

Consultez AWS applications gérées la section pour savoir quelles applications AWS gérées prennent en charge les instances de compte d'IAM Identity Center. Vérifiez la disponibilité de la création d'instances de compte avec votre application AWS gérée.

Activer les instances de compte dans la console IAM Identity Center

Si vous avez activé IAM Identity Center avant le 15 novembre 2023, vous disposez d'une instance organisationnelle d'IAM Identity Center et la possibilité pour les comptes membres de créer des instances de compte est désactivée par défaut. Vous pouvez choisir si vos comptes membres peuvent créer des instances de compte en activant la fonctionnalité d'instance de compte dans le AWS Management Console.

> **Note**
>
> Les comptes membres peuvent créer une instance de compte tant que vous n'avez pas déployé d'instance d'IAM Identity Center dans votre organisation dans une région optionnelle (désactivée par défaut), quelle Région AWS que soit la date de déploiement. Toute instance organisationnelle d'IAM Identity Center déployée dans le cadre d'un opt-in Région AWS empêchera la création d'instances de compte. Pour plus d'informations sur les régions, consultezAWS IAM Identity Center Disponibilité de la région.

Pour permettre la création d'instances de compte par les comptes membres de votre organisation

1. Ouvrez la console IAM Identity Center.
2. Choisissez Paramètres, puis sélectionnez l'onglet Gestion.
3. Dans la section Instances de compte d'IAM Identity Center, choisissez Activer les instances de compte d'IAM Identity Center.

4. Dans la boîte de dialogue Activer les instances de compte d'IAM Identity Center, confirmez que vous souhaitez autoriser les comptes membres de votre organisation à créer des instances de compte en choisissant Activer.

> **Important**
>
> L'activation des instances de compte d'IAM Identity Center pour les comptes des membres est une opération unique. Cela signifie que cette opération ne peut pas être annulée. Une fois activée, vous pouvez limiter la création d'instances de compte en créant une politique de contrôle des services (SCP). Pour obtenir des instructions, consultez la section Contrôle de la création d'instances de compte à l'aide des politiques de contrôle des services.

Contrôlez la création d'instances de compte avec les politiques de contrôle des services

Les utilisateurs peuvent créer une instance d'IAM Identity Center liée à une instance unique Compte AWS, appelée instance de compte d'IAM Identity Center. Vous pouvez contrôler la création d'instances de compte à l'aide des politiques de contrôle des services (SCP).

1. Ouvrez la console IAM Identity Center.
2. Sur le tableau de bord, dans la section Gestion centrale, cliquez sur le bouton Empêcher les instances de compte.
3. Dans la boîte de dialogue Attacher un SCP pour empêcher la création de nouvelles instances de compte, un SCP vous est fourni. Copiez le SCP et cliquez sur le bouton Accéder au tableau de bord du SCP. Vous serez dirigé vers la AWS Organizations console pour créer le SCP ou le joindre sous forme de déclaration à un SCP existant.

   Les politiques de contrôle des services sont une fonctionnalité de AWS Organizations. Pour obtenir des instructions sur la connexion d'un SCP, consultez les politiques de contrôle de service relatives à l'attachement et au détachement du guide de l'AWS Organizations utilisateur.

Plutôt que d'empêcher la création d'instances de compte, vous pouvez limiter la création d'instances de compte à une instance spécifique Compte AWS au sein de votre organisation :

Example : SCP pour contrôler la création d'instances

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

Création d'une instance de compte d'IAM Identity Center

Une instance d'organisation est la principale méthode recommandée pour activer IAM Identity Center. Assurez-vous que votre cas d'utilisation prend en charge la création d'une instance de compte et que vous êtes conscient des considérations à prendre en compte.

Création d'une instance de compte à partir du compte d'un membre de l'organisation ou d'un compte autonome Compte AWS

1. Procédez de l'une des manières suivantes pour vous connecter au AWS Management Console.
   - Nouvel utilisateur AWS (utilisateur root) : connectez-vous en tant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.
   - Vous utilisez déjà AWS (informations d'identification IAM) : connectez-vous à l'aide de vos informations d'identification IAM avec des autorisations administratives.
2. Ouvrez la console IAM Identity Center.
3. Sous Activer le centre d'identité IAM, sélectionnez Activer.
4. Sélectionnez Continuer à créer l'instance de compte, puis choisissez Continuer.

> **Note**
>
> S'il existe une instance organisationnelle d'IAM Identity Center, assurez-vous que votre cas d'utilisation nécessite sa propre instance de compte d'IAM Identity Center. Si ce n'est pas le cas, choisissez Annuler et utilisez l'instance d'organisation.

5. Facultatif. Ajoutez les balises que vous souhaitez associer à cette instance de compte.

Une notification dans la console indique qu'une instance de compte a été créée avec succès et inclut l'ID de l'instance. Vous pouvez nommer votre instance dans le résumé des paramètres.

> **Note**
>
> L'authentification multifactorielle (MFA) est activée par défaut pour les instances de compte. Les utilisateurs sont invités à se connecter à l'aide de la MFA lorsque leur appareil, leur navigateur ou leur emplacement changent. En tant que bonne pratique en matière de sécurité, nous recommandons vivement l'authentification multifacteur pour les identités de vos employés. En savoir plus sur Gérer les appareils MFA dans IAM Identity Center.

Les fonctionnalités de gestion telles que la confirmation de votre source d'identité, le réglage des paramètres d'authentification multifactorielle et l'ajout d'applications AWS gérées doivent être effectuées dans la console IAM Identity Center.

Authentification

Un utilisateur se connecte au portail d' AWS accès à l'aide de son nom d'utilisateur. Dans ce cas, IAM Identity Center redirige la demande vers le service d'authentification IAM Identity Center en fonction du répertoire associé à l'adresse e-mail de l'utilisateur. Une fois authentifiés, les utilisateurs disposent d'un accès par authentification unique à tous les AWS comptes et applications tierces (software-as-a-service SaaS) qui apparaissent sur le portail sans qu'il soit nécessaire de les inviter à se connecter. Cela signifie que les utilisateurs n'ont plus besoin de suivre les informations d'identification de plusieurs comptes pour les différentes AWS applications assignées qu'ils utilisent quotidiennement.

Sessions d'authentification

Il existe deux types de sessions d'authentification gérées par IAM Identity Center : l'une pour représenter la connexion des utilisateurs à IAM Identity Center, et l'autre pour représenter l'accès des utilisateurs aux applications AWS gérées, telles qu'Amazon SageMaker Studio ou Amazon Managed Grafana. Chaque fois qu'un utilisateur se connecte à IAM Identity Center, une session de connexion est créée pour la durée configurée dans IAM Identity Center, qui peut aller jusqu'à 90 jours. Pour plus d'informations, consultez Gérez la durée de session du portail d' AWS accès et des applications intégrées d'IAM Identity Center. Chaque fois que l'utilisateur accède à une application, la session de connexion IAM Identity Center est utilisée pour obtenir une session d'application IAM Identity Center pour cette application. Les sessions d'application IAM Identity Center ont une durée de vie actualisable d'une heure, c'est-à-dire que les sessions d'application IAM Identity Center sont automatiquement actualisées toutes les heures tant que la session de connexion IAM Identity Center à partir de laquelle elles ont été obtenues est toujours valide. Lorsque l'utilisateur utilise IAM Identity Center pour accéder à la CLI AWS Management Console ou à la CLI, la session de connexion IAM Identity Center est utilisée pour obtenir une session IAM, comme indiqué dans le jeu d'autorisations IAM Identity Center correspondant (plus précisément, IAM Identity Center assume un rôle IAM, géré par IAM Identity Center, dans le compte cible).

Lorsque vous désactivez ou supprimez un utilisateur dans IAM Identity Center, cet utilisateur est immédiatement empêché de se connecter pour créer de nouvelles sessions de connexion IAM Identity Center. Les sessions de connexion IAM Identity Center sont mises en cache pendant une heure, ce qui signifie que lorsque vous désactivez ou supprimez un utilisateur alors qu'il possède une session de connexion IAM Identity Center active, sa session de connexion IAM Identity Center existante se poursuit pendant une heure au maximum, selon la date à laquelle la session de

connexion a été actualisée pour la dernière fois. Pendant ce temps, l'utilisateur peut lancer de nouvelles sessions d'application IAM Identity Center et de rôle IAM.

Une fois la session de connexion IAM Identity Center expirée, l'utilisateur ne peut plus lancer de nouvelles sessions d'application IAM Identity Center ou de nouvelles sessions de rôle IAM. Toutefois, les sessions d'application IAM Identity Center peuvent également être mises en cache pendant une heure au maximum, de sorte que l'utilisateur peut conserver l'accès à une application jusqu'à une heure après l'expiration de la session de connexion IAM Identity Center. Toutes les sessions de rôle IAM existantes se poursuivront en fonction de la durée configurée dans le jeu d'autorisations IAM Identity Center (configurable par l'administrateur, jusqu'à 12 heures).

Le tableau ci-dessous récapitule ces comportements :

Expérience utilisateur/comportement du système	Durée après la désactivation/suppression de l'utilisateur
L'utilisateur ne peut plus se connecter à IAM Identity Center ; il ne peut pas obtenir une nouvelle session de connexion à IAM Identity Center	Aucune (en vigueur immédiatement)
L'utilisateur ne peut plus démarrer de nouvelles sessions d'application ou de rôle IAM via IAM Identity Center	Jusqu'à 1 heure
L'utilisateur ne peut plus accéder à aucune application (toutes les sessions d'application sont terminées)	Jusqu'à 2 heures (jusqu'à 1 heure pour l'expiration de la session de connexion IAM Identity Center, plus 1 heure pour l'expiration de la session d'application IAM Identity Center)
L'utilisateur ne peut plus y accéder Comptes AWS via IAM Identity Center	Jusqu'à 13 heures (jusqu'à 1 heure pour l'expiration de la session de connexion IAM Identity Center, plus jusqu'à 12 heures pour l'expiration de la session de rôle IAM configurée par l'administrateur, conformément aux paramètres de durée de session IAM Identity Center définis pour l'ensemble d'autorisations)

Pour en savoir plus sur les sessions, consultez Définir la durée de la session.

Gérez les identités du personnel

AWS Identity and Access Management(IAM) vous aide à gérer en toute sécurité les identités et l'accès aux AWS services et aux ressources. En tant que service IAM, AWS IAM Identity Center vous pouvez créer ou connecter les identités de vos employés en AWS une seule fois et gérer l'accès de manière centralisée à vos multiples Comptes AWS applications.

Pour les clients d'IAM Identity Center, il n'y a aucun changement dans la façon dont vous gérez de manière centralisée l'accès à plusieurs applications Comptes AWS ou applications. Pour les nouveaux clients d'IAM Identity Center, vous pouvez configurer de manière flexible IAM Identity Center pour qu'il fonctionne parallèlement ou remplace la gestion d'Compte AWSaccès unique à l'aide d'IAM.

Rubriques

Cas d'utilisation

Vous trouverez ci-dessous des cas d'utilisation qui montrent comment vous pouvez utiliser IAM Identity Center pour répondre aux différents besoins de l'entreprise.

Rubriques

Activez l'accès par authentification unique à vos AWS applications (rôle d'administrateur des applications)

Ce cas d'utilisation fournit des conseils si vous êtes un administrateur d'applications qui gère des applications AWS applications gérées telles qu'Amazon SageMaker ou AWS IoT SiteWise si vous devez fournir un accès par authentification unique à vos utilisateurs.

Avant de commencer, tenez compte des points suivants :

- Voulez-vous créer un environnement de test ou de production dans une organisation distincte dans AWS Organizations ?
- Le centre d'identité IAM est-il déjà activé dans votre organisation ? Êtes-vous autorisé à activer IAM Identity Center dans le compte de gestion de AWS Organizations ?

Consultez les conseils suivants pour déterminer les prochaines étapes en fonction des besoins de votre entreprise.

Configurer mon AWS application en mode autonome Compte AWS

Si vous devez fournir un accès par authentification unique à une AWS application et que vous savez que votre service informatique n'utilise pas encore IAM Identity Center, vous devrez peut-être créer un centre autonome Compte AWS pour commencer. Par défaut, lorsque vous créez la vôtreCompte AWS, vous disposez des autorisations nécessaires pour créer et gérer votre propre AWS organisation. Pour activer IAM Identity Center, vous devez disposer d'Utilisateur racine d'un compte AWSautorisations.

IAM Identity Center AWS Organizations peut être activé automatiquement lors de la configuration de certaines AWS applications (par exemple, Amazon Managed Grafana). Si votre AWS application ne permet pas d'activer ces services, vous devez configurer AWS Organizations un centre d'identité IAM avant de pouvoir fournir un accès par authentification unique à votre application.

Le centre d'identité IAM n'est pas configuré dans mon organisation

En tant qu'administrateur d'applications, il se peut que vous ne puissiez pas activer IAM Identity Center, en fonction de vos autorisations. IAM Identity Center nécessite des autorisations spécifiques dans le compte AWS Organizations de gestion. Dans ce cas, contactez l'administrateur approprié pour activer IAM Identity Center dans le compte de gestion des Organizations.

Si vous disposez des autorisations suffisantes pour activer IAM Identity Center, faites-le d'abord, puis procédez à la configuration de l'application. Pour plus d'informations, consultez Démarrez avec les tâches courantes dans IAM Identity Center.

Le centre d'identité IAM est actuellement configuré dans mon organisation

Dans ce scénario, vous pouvez continuer à déployer votre AWS application sans effectuer d'autre action.

> **Note**
>
> Si votre organisation a activé IAM Identity Center dans le compte de gestion avant le 25 novembre 2019, vous devez également activer les applications AWS gérées dans le compte de gestion et éventuellement dans les comptes des membres. Si vous les activez uniquement dans le compte de gestion, vous pourrez les activer ultérieurement dans les comptes membres. Pour activer ces applications, choisissez Activer l'accès sur la page Paramètres de la console IAM Identity Center, dans la section des applications AWS gérées. Pour plus d'informations, consultez Configuration d'IAM Identity Center pour partager les informations d'identité .

Activez l'accès par authentification unique à vos instances Windows Amazon EC2

Vous pouvez activer l'accès par authentification unique à vos instances Windows Amazon EC2 si vous êtes un administrateur d'applications qui gère les utilisateurs dans le répertoire Identity Center (la source d'identité par défaut pour IAM Identity Center) ou un fournisseur d'identité externe (IdP) compatible, et vous devez fournir à IAM Identity Center un accès à vos bureaux Windows Amazon EC2 depuis la console Fleet Manager. AWS

Avec cette configuration, vous pouvez accéder en toute sécurité à vos instances Windows Amazon EC2 avec les informations d'identification d'entreprise existantes. Vous n'avez pas besoin de partager les informations d'identification de l'administrateur, d'accéder à plusieurs reprises aux informations d'identification ou de configurer le logiciel client d'accès à distance. Vous pouvez accorder et révoquer de manière centralisée l'accès à vos instances Windows Amazon EC2 à grande échelle sur plusieurs instances. Comptes AWS Par exemple, si vous supprimez un employé de votre source d'identité intégrée IAM Identity Center, il perd automatiquement l'accès à toutes les AWS ressources, y compris aux instances Windows Amazon EC2.

Pour plus d'informations, consultez Comment activer l'authentification unique sécurisée et fluide sur les instances Windows Amazon EC2 avec IAM Identity Center.

Pour une démonstration de la configuration d'IAM Identity Center afin d'activer cette fonctionnalité, consultez Activation de l'authentification unique sur Amazon EC2 Windows avec IAM Identity Center.

Utilisateurs, groupes et provisionnement

Tenez compte des considérations suivantes lorsque vous travaillez avec des utilisateurs et des groupes dans IAM Identity Center.

Unicité du nom d'utilisateur et de l'adresse e-mail

Les utilisateurs d'IAM Identity Center doivent être identifiables de manière unique. IAM Identity Center implémente un nom d'utilisateur qui est l'identifiant principal de vos utilisateurs. Bien que la plupart des utilisateurs définissent le nom d'utilisateur comme l'adresse e-mail d'un utilisateur, IAM Identity Center et la norme SAML 2.0 ne l'exigent pas. Cependant, de nombreuses applications basées sur SAML 2.0 utilisent une adresse e-mail comme identifiant unique pour les utilisateurs. Ces applications obtiennent ces informations à partir d'assertions envoyées par un fournisseur d'identité SAML 2.0 lors de l'authentification. Ces applications dépendent de l'unicité des adresses e-mail de chaque utilisateur. Pour cette raison, IAM Identity Center vous permet de spécifier autre chose qu'une adresse e-mail pour la connexion des utilisateurs. IAM Identity Center exige que tous les noms d'utilisateur et adresses e-mail de vos utilisateurs soient uniques et non nuls.

Groups

Les groupes sont une combinaison logique d'utilisateurs que vous définissez. Vous pouvez créer des groupes et y ajouter des utilisateurs. IAM Identity Center ne prend pas en charge l'ajout d'un groupe à un groupe (groupes imbriqués). Les groupes sont utiles lors de l'attribution de l'accès aux applications Comptes AWS et de leur attribution. Plutôt que d'attribuer des autorisations à chaque utilisateur individuellement, vous accordez des autorisations à un groupe. Plus tard, lorsque vous ajoutez ou supprimez des utilisateurs d'un groupe, l'utilisateur obtient ou perd l'accès dynamique aux comptes et aux applications que vous avez affectés au groupe.

Provisionnement d'utilisateurs et de groupes

Le provisionnement est le processus qui consiste à mettre les informations des utilisateurs et des groupes à la disposition d'IAM Identity Center et des applications AWS gérées ou des applications

gérées par le client. Vous pouvez créer des utilisateurs et des groupes directement dans IAM Identity Center, ou travailler avec les utilisateurs et les groupes que vous avez dans Active Directory ou avec un fournisseur d'identité externe. Avant de pouvoir utiliser IAM Identity Center pour attribuer aux utilisateurs et aux groupes des autorisations d'accès dans unCompte AWS, IAM Identity Center doit connaître les utilisateurs et les groupes. De même, les applications AWS gérées et les applications gérées par le client peuvent fonctionner avec des utilisateurs et des groupes dont IAM Identity Center a connaissance.

Le provisionnement dans IAM Identity Center varie en fonction de la source d'identité que vous utilisez. Pour plus d'informations, consultez Gérez votre source d'identité.

Gérez votre source d'identité

Votre source d'identité dans IAM Identity Center définit l'endroit où vos utilisateurs et vos groupes sont gérés. Après avoir configuré votre source d'identité, vous pouvez rechercher des utilisateurs ou des groupes pour leur accorder un accès par authentification unique aux Comptes AWS applications, ou les deux.

Vous ne pouvez avoir qu'une seule source d'identité par organisation dansAWS Organizations. Vous pouvez choisir l'une des sources d'identité suivantes :

- Répertoire du centre d'identité : lorsque vous activez IAM Identity Center pour la première fois, il est automatiquement configuré avec un répertoire du centre d'identité comme source d'identité par défaut. C'est ici que vous créez vos utilisateurs et vos groupes, et que vous attribuez leur niveau d'accès à vos applications Comptes AWS et à vos applications.
- Active Directory : choisissez cette option si vous souhaitez continuer à gérer les utilisateurs de votre AWS Managed Microsoft AD annuaire en utilisant AWS Directory Service ou de votre annuaire autogéré dansActive Directory (AD).
- Fournisseur d'identité externe : choisissez cette option si vous souhaitez gérer les utilisateurs dans un fournisseur d'identité externe (IdP) tel que Okta ou. Microsoft Entra ID

> **Note**
>
> IAM Identity Center ne prend pas en charge Simple AD basé sur Samba4 en tant que source d'identité.

Rubriques

Considérations relatives à la modification de votre source d'identité

Bien que vous puissiez modifier votre source d'identité à tout moment, nous vous recommandons de réfléchir à l'impact de cette modification sur votre déploiement actuel.

Si vous gérez déjà des utilisateurs et des groupes dans une source d'identité, le passage à une autre source d'identité peut supprimer toutes les attributions d'utilisateurs et de groupes que vous avez configurées dans IAM Identity Center. Dans ce cas, tous les utilisateurs, y compris l'utilisateur administratif d'IAM Identity Center, perdront l'accès par authentification unique à leurs applications Comptes AWS et à leurs applications.

Avant de modifier la source d'identité pour IAM Identity Center, prenez en compte les points suivants avant de poursuivre. Si vous souhaitez continuer à modifier votre source d'identité, reportez-vous à la section Changez votre source d'identité pour plus d'informations.

Passage d'IAM Identity Center à Active Directory

Si vous gérez déjà des utilisateurs et des groupes dans Active Directory, nous vous recommandons d'envisager de connecter votre annuaire lorsque vous activez IAM Identity Center et que vous choisissez votre source d'identité. Faites-le avant de créer des utilisateurs et des groupes dans le répertoire par défaut d'Identity Center et de procéder à des affectations.

Si vous gérez déjà des utilisateurs et des groupes dans le répertoire par défaut d'Identity Center, tenez compte des points suivants :

- Attributions supprimées et utilisateurs et groupes supprimés : le fait de remplacer votre source d'identité par Active Directory supprime vos utilisateurs et vos groupes de l'annuaire Identity Center. Cette modification supprime également vos assignations. Dans ce cas, une fois que vous

êtes passé à Active Directory, vous devez synchroniser vos utilisateurs et vos groupes depuis Active Directory vers le répertoire Identity Center, puis réappliquer leurs attributions.

Si vous choisissez de ne pas utiliser Active Directory, vous devez créer vos utilisateurs et groupes dans le répertoire Identity Center, puis effectuer des assignations.

- Les attributions ne sont pas supprimées lorsque les identités sont supprimées : lorsque les identités sont supprimées dans le répertoire Identity Center, les attributions correspondantes sont également supprimées dans IAM Identity Center. Toutefois, dans Active Directory, lorsque des identités sont supprimées (que ce soit dans Active Directory ou dans les identités synchronisées), les attributions correspondantes ne sont pas supprimées.
- Aucune synchronisation sortante pour les API : si vous utilisez Active Directory comme source d'identité, nous vous recommandons d'utiliser les API de création, de mise à jour et de suppression avec prudence. IAM Identity Center ne prend pas en charge la synchronisation sortante. Par conséquent, votre source d'identité n'est pas automatiquement mise à jour avec les modifications que vous apportez aux utilisateurs ou aux groupes à l'aide de ces API.
- L'URL du portail d'accès va changer — La modification de votre source d'identité entre IAM Identity Center et Active Directory modifie également l'URL du portail AWS d'accès.

Pour plus d'informations sur la manière dont IAM Identity Center approvisionne les utilisateurs et les groupes, consultezSe connecter à un Microsoft AD annuaire.

Passage d'IAM Identity Center à un IdP externe

Si vous remplacez votre source d'identité d'IAM Identity Center par un fournisseur d'identité externe (IdP), tenez compte des points suivants :

- Les assignations et les adhésions fonctionnent avec des assertions correctes : vos assignations d'utilisateur, vos assignations de groupe et vos appartenances à des groupes continueront de fonctionner tant que le nouvel IdP envoie les assertions correctes (par exemple, les NameID SAML). Ces assertions doivent correspondre aux noms d'utilisateur et aux groupes d'IAM Identity Center.
- Aucune synchronisation sortante : IAM Identity Center ne prend pas en charge la synchronisation sortante. Votre IdP externe ne sera donc pas automatiquement mis à jour en fonction des modifications apportées aux utilisateurs et aux groupes dans IAM Identity Center.
- Provisionnement SCIM : si vous utilisez le provisionnement SCIM, les modifications apportées aux utilisateurs et aux groupes de votre fournisseur d'identité ne sont reflétées dans IAM Identity

Center qu'une fois que celui-ci a envoyé ces modifications à IAM Identity Center. veuillez consulter Considérations relatives à l'utilisation du provisionnement automatique.

- Annulation : vous pouvez à tout moment rétablir votre source d'identité pour qu'elle utilise à nouveau IAM Identity Center. veuillez consulter Passage d'un IdP externe à IAM Identity Center.

Pour plus d'informations sur la manière dont IAM Identity Center approvisionne les utilisateurs et les groupes, consultezConnectez-vous à un fournisseur d'identité externe.

Passage d'un IdP externe à IAM Identity Center

Si vous remplacez votre source d'identité par un fournisseur d'identité externe (IdP) par IAM Identity Center, tenez compte des points suivants :

- IAM Identity Center préserve toutes vos assignations.
- Forcer la réinitialisation du mot de passe — Les utilisateurs qui possédaient des mots de passe dans IAM Identity Center peuvent continuer à se connecter avec leurs anciens mots de passe. Pour les utilisateurs qui se trouvaient dans l'IdP externe et non dans IAM Identity Center, un administrateur doit forcer la réinitialisation du mot de passe.

Pour plus d'informations sur la manière dont IAM Identity Center approvisionne les utilisateurs et les groupes, consultezGestion des identités dans IAM Identity Center.

Passage d'un IdP externe à un autre IdP externe

Si vous utilisez déjà un IdP externe comme source d'identité pour IAM Identity Center et que vous passez à un autre IdP externe, tenez compte des points suivants :

- Les assignations et les adhésions fonctionnent avec des assertions correctes. IAM Identity Center conserve toutes vos assignations. Les attributions d'utilisateurs, les attributions de groupes et les appartenances à des groupes continueront de fonctionner tant que le nouvel IdP envoie les assertions correctes (par exemple, les NameID SAML).

  Ces assertions doivent correspondre aux noms d'utilisateur dans IAM Identity Center lorsque vos utilisateurs s'authentifient via le nouvel IdP externe.
- Provisionnement du SCIM : si vous utilisez le SCIM pour le provisionnement dans IAM Identity Center, nous vous recommandons de consulter les informations spécifiques à l'IdP contenues dans ce guide et la documentation fournie par l'IdP afin de vous assurer que le nouveau fournisseur fera correspondre correctement les utilisateurs et les groupes lorsque le SCIM sera activé.

Pour plus d'informations sur la manière dont IAM Identity Center approvisionne les utilisateurs et les groupes, consultezConnectez-vous à un fournisseur d'identité externe.

Passage d'Active Directory à un IdP externe

Si vous remplacez votre source d'identité par un IdP externe par Active Directory, ou d'Active Directory par un IdP externe, tenez compte des points suivants :

- Les utilisateurs, les groupes et les attributions sont supprimés : tous les utilisateurs, groupes et attributions sont supprimés d'IAM Identity Center. Aucune information d'utilisateur ou de groupe n'est affectée ni dans l'IdP externe ni dans Active Directory.
- Approvisionnement des utilisateurs : si vous passez à un IdP externe, vous devez configurer IAM Identity Center pour approvisionner vos utilisateurs. Vous devez également configurer manuellement les utilisateurs et les groupes pour l'IdP externe avant de pouvoir configurer les attributions.
- Création d'attributions et de groupes : si vous passez à Active Directory, vous devez créer des attributions avec les utilisateurs et les groupes figurant dans votre annuaire dans Active Directory.

Pour plus d'informations sur la manière dont IAM Identity Center approvisionne les utilisateurs et les groupes, consultezSe connecter à un Microsoft AD annuaire.

Changez votre source d'identité

La procédure suivante explique comment passer d'un répertoire fourni par IAM Identity Center (le répertoire du centre d'identité par défaut) à Active Directory ou à un fournisseur d'identité externe, ou inversement. Avant de continuer, veuillez consulter les informations dansConsidérations relatives à la modification de votre source d'identité. En fonction de votre déploiement actuel, cette modification peut supprimer toutes les attributions d'utilisateurs et de groupes que vous avez configurées dans IAM Identity Center. Dans ce cas, tous les utilisateurs, y compris l'utilisateur administratif dans IAM Identity Center, perdront l'accès par authentification unique à leurComptes AWSet applications.

Pour modifier votre source d'identité

1. Ouvrir leConsole IAM Identity Center.
2. Sélectionnez Settings (Paramètres).
3. Sur leParamètrespage, choisissez leIdentité sourceonglet. ChoisissezActions, puisChanger de source d'identité.

4. SousChoisir une identité source, sélectionnez la source que vous souhaitez modifier, puisSuivant.

   Si vous passez à Active Directory, choisissez le répertoire disponible dans le menu de la page suivante.

   > **Important**
   >
   > La modification de votre référentiel d'identité vers ou depuis Active Directory supprime les utilisateurs et les groupes du répertoire Identity Center. Cette modification supprime également toutes les attributions que vous avez configurées dans IAM Identity Center.

   Si vous passez à un fournisseur d'identité externe, nous vous recommandons de suivre les étapes décrites dansComment se connecter à un fournisseur d'identité externe.

5. Une fois que vous avez lu l'avertissement et que vous êtes prêt à continuer, tapezACCEPTER.
6. ChoisissezChanger de source d'identité. Si vous remplacez votre identité source d'identité en mode Active Directory, passez à l'étape suivante.
7. En remplaçant votre référentiel d'identité par Active Directory, vous accédez auParamètrespage. Sur leParamètrespage, procédez de l'une des manières suivantes :

   - ChoisissezDémarrer une configuration guidée. Pour plus d'informations sur la procédure de configuration guidée, consultezConfiguration guidée.
   - Dans leIdentité sourcesection, choisissezActions, puisGérer la synchronisation avecpour configurer votreportée de synchronisation avec, la liste des utilisateurs et des groupes à synchroniser.

Gérez la connexion et l'utilisation des attributs pour tous les types de sources d'identité

IAM Identity Center fournit les fonctionnalités suivantes qui permettent aux administrateurs de contrôler l'utilisation du portail d' AWS accès, de définir la durée des sessions pour les utilisateurs du portail d' AWS accès et de vos applications, et d'utiliser des attributs pour le contrôle d'accès. Ces fonctionnalités fonctionnent avec un annuaire Identity Center ou un fournisseur d'identité externe comme source d'identité.

> **Note**
>
> Si vous utilisez Active Directory comme source d'identité pour IAM Identity Center, la gestion de session n'est pas prise en charge.

Rubriques

- Gérez la durée de session du portail d' AWS accès et des applications intégrées d'IAM Identity Center
- Configurer la durée de session du portail d' AWS accès et des applications intégrées d'IAM Identity Center
- Supprimer des sessions pour le portail AWS d'accès et les applications AWS intégrées
- Attributs d'utilisateur et de groupe pris en charge

Gérez la durée de session du portail d' AWS accès et des applications intégrées d'IAM Identity Center

L'administrateur du centre d'identité IAM peut configurer la durée de session pour les applications intégrées à IAM Identity Center et le. Portail d'accès AWS La configuration de la durée des sessions détermine la fréquence à laquelle les utilisateurs doivent se réauthentifier. L'administrateur du centre d'identité IAM peut mettre fin à une session active du portail d' AWS accès et, ce faisant, également mettre fin aux sessions des applications intégrées.

Pour plus d'informations, consultez Configurer la durée de session du portail d' AWS accès et des applications intégrées d'IAM Identity Center. Pour plus d'informations sur la gestion et les sessions des utilisateurs finaux, consultezSupprimer des sessions pour le portail AWS d'accès et les applications AWS intégrées.

> **Note**
>
> La modification de la AWS durée de session du portail d' AWS accès et la fin des sessions du portail d'accès n'ont aucun effet sur la durée de session de la console de AWS gestion que vous définissez dans vos ensembles d'autorisations.

Configurer la durée de session du portail d' AWS accès et des applications intégrées d'IAM Identity Center

La durée de session d'authentification dans les applications intégrées Portail d'accès AWS et IAM Identity Center est la durée maximale pendant laquelle un utilisateur peut se connecter sans se réauthentifier. La durée de session par défaut est de 8 heures. L'administrateur du centre d'identité IAM peut spécifier une durée différente, allant d'un minimum de 15 minutes à un maximum de 90 jours. Pour plus d'informations sur la durée des sessions d'authentification et le comportement des utilisateurs, consultezAuthentification.

Les rubriques suivantes fournissent des informations sur la configuration de la durée de session du portail d' AWS accès et des applications intégrées d'IAM Identity Center.

Rubriques

Prérequis et considérations

Voici les conditions préalables et les considérations relatives à la configuration de la durée de session pour le portail AWS d'accès et les applications intégrées d'IAM Identity Center.

Fournisseurs d'identité externes

IAM Identity Center utilise les `SessionNotOnOrAfter` attributs des assertions SAML pour déterminer la durée de validité de la session.

- Si `SessionNotOnOrAfter` aucune assertion SAML n'est transmise, la durée d'une session du portail d' AWS accès n'est pas affectée par la durée de votre session IdP externe. Par exemple, si la durée de votre session IdP est de 24 heures et que vous définissez une durée de session de 18 heures dans IAM Identity Center, vos utilisateurs doivent s'authentifier à nouveau sur le AWS portail d'accès après 18 heures.
- Si une assertion SAML `SessionNotOnOrAfter` est transmise, la valeur de durée de session est définie sur la durée la plus courte entre la durée de session du portail d' AWS accès et la durée de votre session IdP SAML. Si vous définissez une durée de session de 72 heures dans IAM Identity Center et que votre IdP a une durée de session de 18 heures, vos utilisateurs auront accès aux AWS ressources pendant les 18 heures définies dans votre IdP.

- Si la durée de session de votre IdP est plus longue que celle définie dans IAM Identity Center, vos utilisateurs pourront démarrer une nouvelle session IAM Identity Center sans avoir à saisir à nouveau leurs informations d'identification, sur la base de leur session de connexion toujours valide avec votre IdP.

> **Note**
>
> Si vous utilisez Active Directory comme source d'identité pour IAM Identity Center, la gestion de session n'est pas prise en charge.

AWS CLI et sessions SDK

Si vous utilisez des kits de AWS Command Line Interface développement AWS logiciel (SDK) ou d'autres outils de AWS développement pour accéder aux AWS services par programmation, les conditions préalables suivantes doivent être remplies pour définir la durée de session pour le portail d' AWS accès et les applications intégrées IAM Identity Center.

- Vous devez configurer la durée de session du portail d' AWS accès dans la console IAM Identity Center.
- Vous devez définir un profil pour les paramètres d'authentification unique dans votre fichier de AWS configuration partagé. Ce profil est utilisé pour se connecter au portail AWS d'accès. Nous vous recommandons d'utiliser la configuration du fournisseur de jetons SSO. Avec cette configuration, votre AWS SDK ou outil peut récupérer automatiquement des jetons d'authentification actualisés. Pour plus d'informations, consultez la section Configuration du fournisseur de jetons SSO dans le Guide de référence du AWS SDK et des outils.
- Les utilisateurs doivent exécuter une version du AWS CLI ou un SDK qui prend en charge la gestion des sessions.

Versions minimales du AWS CLI qui prennent en charge la gestion des sessions

Vous trouverez ci-dessous les versions minimales AWS CLI qui prennent en charge la gestion des sessions.

- AWS CLI V2 2.9 ou version ultérieure
- AWS CLI V1 1.27.10 ou version ultérieure

Pour plus d'informations sur l'installation ou la mise à jour de la dernière AWS CLI version, voir Installation ou mise à jour de la dernière version du AWS CLI.

Si vos utilisateurs exécutent le AWS CLI, si vous actualisez votre ensemble d'autorisations juste avant l'expiration de la session IAM Identity Center et que la durée de la session est fixée à 20 heures alors que la durée de l'ensemble d'autorisations est fixée à 12 heures, la AWS CLI session dure au maximum 20 heures plus 12 heures pour un total de 32 heures. Pour plus d'informations sur la CLI IAM Identity Center, consultez la section AWS CLI Command Reference.

Versions minimales des SDK prenant en charge la gestion des sessions IAM Identity Center

Vous trouverez ci-dessous les versions minimales des SDK qui prennent en charge la gestion des sessions IAM Identity Center.

SDK	Version minimale
Python	1,26,10
PHP	3,245,0
Ruby	aws-sdk-core 3,167,0
Java V2	AWS SDK pour Java v2 (2.18.13)
Go V2	SDK complet : version 011-11 et modules Go spécifiques : credentials/v1.13.0, config/v1.18.0
JS V2	2,1253,0
JS V3	version 3.210.0
C++	1,9,372
.NET	v3.7.400.0

Comment configurer la durée de session

Utilisez la procédure suivante pour configurer la durée de session du portail d' AWS accès et des applications intégrées d'IAM Identity Center.

1. Ouvrez la console IAM Identity Center.

2. Sélectionnez Settings (Paramètres).
3. Sur la page Paramètres, choisissez l'onglet Authentification.
4. Sous Authentification, à côté de Paramètres de session, choisissez Configurer. La boîte de dialogue Configurer les paramètres de session apparaît.
5. Dans la boîte de dialogue Configurer les paramètres de session, choisissez la durée maximale de session en minutes, heures et jours pour vos utilisateurs en sélectionnant la flèche déroulante. Choisissez la durée de la session, puis cliquez sur Enregistrer. Vous revenez à la page des paramètres.

Supprimer des sessions pour le portail AWS d'accès et les applications AWS intégrées

Utilisez la procédure suivante pour afficher et supprimer les sessions actives d'un utilisateur d'IAM Identity Center.

Pour supprimer une session active du portail d' AWS accès et des applications intégrées d'IAM Identity Center

1. Ouvrez la console IAM Identity Center.
2. Choisissez Utilisateurs.
3. Sur la page Utilisateurs, choisissez le nom d'utilisateur de l'utilisateur dont vous souhaitez gérer les sessions. Cela vous amène à une page contenant les informations de l'utilisateur.
4. Sur la page de l'utilisateur, choisissez l'onglet Sessions actives. Le nombre entre parenthèses à côté de Sessions actives indique le nombre de sessions actives en cours pour cet utilisateur.
5. Cochez les cases à côté des sessions que vous souhaitez supprimer, puis choisissez Supprimer la session. Une boîte de dialogue apparaît pour confirmer que vous supprimez des sessions actives pour cet utilisateur. Lisez les informations de la boîte de dialogue et si vous souhaitez continuer, choisissez Supprimer la session.
6. Vous êtes renvoyé sur la page de l'utilisateur. Une barre clignotante verte apparaît pour indiquer que les sessions sélectionnées ont été correctement supprimées.

Pour plus d'informations sur le comportement des sessions d'authentification révoquées, consultezSessions d'authentification.

Attributs d'utilisateur et de groupe pris en charge

Les attributs sont des informations qui vous aident à définir et à identifier des objets d'utilisateur ou de groupe individuelsname, tels queemail, oumembers. IAM Identity Center prend en charge les attributs les plus couramment utilisés, qu'ils soient saisis manuellement lors de la création de l'utilisateur ou lorsqu'ils sont automatiquement provisionnés à l'aide d'un moteur de synchronisation tel que défini dans la spécification du système de gestion des identités interdomaines (SCIM). Pour plus d'informations sur cette spécification, consultez https://tools.ietf.org/html/rfc7642. Pour plus d'informations sur le provisionnement manuel et automatique, consultezProvisionnement lorsque les utilisateurs proviennent d'un IdP externe.

Comme IAM Identity Center prend en charge le SCIM pour les cas d'utilisation du provisionnement automatique, le répertoire Identity Center prend en charge tous les attributs d'utilisateur et de groupe répertoriés dans la spécification SCIM, à quelques exceptions près. Les sections suivantes décrivent les attributs qui ne sont pas pris en charge par IAM Identity Center.

Objets utilisateur

Tous les attributs du schéma utilisateur SCIM (https://tools.ietf.org/html/rfc7643#section-8.3) sont pris en charge dans le magasin d'identités IAM Identity Center, à l'exception des suivants :

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

Tous les sous-attributs des utilisateurs sont pris en charge, à l'exception des suivants :

- `'display'`sous-attribut de tout attribut à valeurs multiples (par exemple, `emails` ou) `phoneNumbers`
- `'version'`sous-attribut d'`''meta'`attribut

Objets de groupe

Tous les attributs du schéma de groupe SCIM (https://tools.ietf.org/html/rfc7643#section-8.4) sont pris en charge.

Tous les sous-attributs des groupes sont pris en charge, à l'exception des suivants :

- `'display'` sous-attribut de tout attribut à valeurs multiples (par exemple, membres).

Gestion des identités dans IAM Identity Center

IAM Identity Center fournit les fonctionnalités suivantes à vos utilisateurs et groupes :

- Créer vos utilisateurs et groupes.
- Ajouter vos utilisateurs en tant que membres aux groupes.
- Attribuez aux groupes le niveau d'accès souhaité à vos applications Comptes AWS et à vos applications.

Pour gérer les utilisateurs et les groupes dans le magasin IAM Identity Center, AWS prend en charge les opérations d'API répertoriées dans Identity Center Actions.

Provisionnement lorsque les utilisateurs se trouvent dans IAM Identity Center

Lorsque vous créez des utilisateurs et des groupes directement dans IAM Identity Center, le provisionnement est automatique. Ces identités sont immédiatement disponibles pour être utilisées pour effectuer des assignations et pour être utilisées par les applications. Pour plus d'informations, consultez Provisionnement d'utilisateurs et de groupes.

Modification de la source de votre identité

Si vous préférez gérer les utilisateurs dans AWS Managed Microsoft AD, vous pouvez arrêter d'utiliser votre répertoire Identity Center à tout moment et connecter IAM Identity Center à votre répertoire dans Microsoft AD en utilisant AWS Directory Service. Pour plus d'informations, consultez les considérations relatives àPassage d'IAM Identity Center à Active Directory.

Si vous préférez gérer les utilisateurs dans un fournisseur d'identité externe (IdP), vous pouvez connecter IAM Identity Center à votre IdP et activer le provisionnement automatique. Pour plus d'informations, consultez les considérations relatives àPassage d'IAM Identity Center à un IdP externe.

Rubriques

- Ajout d'utilisateurs
- Ajouter des groupes

- Ajouter des utilisateurs à des groupes
- Supprimer des groupes dans IAM Identity Center
- Supprimer des utilisateurs dans IAM Identity Center
- Désactiver l'accès des utilisateurs dans IAM Identity Center
- Modifier les propriétés de l'utilisateur
- Réinitialisation du mot de passe utilisateur IAM Identity Center pour un utilisateur final
- Envoyer un e-mail OTP pour les utilisateurs créés à partir de l'API
- Exigences relatives aux mots de passe lors de la gestion des identités dans IAM Identity Center

Ajout d'utilisateurs

Les utilisateurs et les groupes que vous créez dans votre répertoire Identity Center ne sont disponibles que dans IAM Identity Center. Utilisez la procédure suivante pour ajouter des utilisateurs à votre répertoire Identity Center à l'aide de la console IAM Identity Center. Vous pouvez également appeler l'opération AWS API CreateUserpour ajouter des utilisateurs.

Pour ajouter un utilisateur

1. Ouvrez la console IAM Identity Center.
2. Choisissez Utilisateurs.
3. Choisissez Ajouter un utilisateur et fournissez les informations requises suivantes :

    a. Nom d'utilisateur — Ce nom d'utilisateur est obligatoire pour se connecter au portail AWS d'accès et ne pourra pas être modifié ultérieurement. Il doit comporter entre 1 et 100 caractères.

    b. Mot de passe — Vous pouvez soit envoyer un e-mail contenant les instructions de configuration du mot de passe (il s'agit de l'option par défaut), soit générer un mot de passe à usage unique. Si vous créez un utilisateur administratif et que vous choisissez d'envoyer un e-mail, assurez-vous de spécifier une adresse e-mail à laquelle vous pouvez accéder.

        i. Envoyez un e-mail à cet utilisateur avec les instructions de configuration du mot de passe. — Cette option envoie automatiquement à l'utilisateur une adresse e-mail provenant d'Amazon Web Services, avec pour objet Invitation to join AWS IAM Identity Center (successeur de Single Sign-On). AWS L'e-mail invite l'utilisateur au nom de votre entreprise à accéder au portail d'accès IAM Identity Center AWS .

> **Note**
>
> Dans certaines régions, IAM Identity Center envoie des e-mails aux utilisateurs utilisant Amazon Simple Email Service depuis une autre Région AWS région. Pour plus d'informations sur le mode d'envoi des e-mails, consultezAppels interrégionaux.
>
> Tous les e-mails envoyés par le service IAM Identity Center proviendront soit de l'adresse`no-reply@signin.aws.com`, soit de. `no-reply@login.awsapps.com` Nous vous recommandons de configurer votre système de messagerie de manière à ce qu'il accepte les e-mails provenant de ces adresses d'expéditeur et qu'il ne les traite pas comme du courrier indésirable ou du spam.

ii. Générez un mot de passe à usage unique que vous pourrez partager avec cet utilisateur. — Cette option vous fournit l'URL du portail AWS d'accès et les détails du mot de passe que vous pouvez envoyer manuellement à l'utilisateur à partir de votre adresse e-mail.

c. Adresse e-mail — L'adresse e-mail doit être unique.

d. Confirmer l'adresse e-mail

e. Prénom : vous devez saisir un nom ici pour que le provisionnement automatique fonctionne. Pour plus d'informations, consultez Approvisionnement automatique.

f. Nom de famille : vous devez saisir un nom ici pour que le provisionnement automatique fonctionne.

g. Display name (Nom d'affichage)

> **Note**
>
> (Facultatif) Le cas échéant, vous pouvez spécifier des valeurs pour des attributs supplémentaires tels que l'identifiant immuable Microsoft 365 de l'utilisateur afin de fournir à l'utilisateur un accès par authentification unique à certaines applications professionnelles.

4. Choisissez Suivant.

5. Le cas échéant, sélectionnez un ou plusieurs groupes auxquels vous souhaitez ajouter l'utilisateur, puis choisissez Next.

6. Passez en revue les informations que vous avez spécifiées pour l'étape 1 : Spécifier les détails de l'utilisateur et pour l'étape 2 : ajouter un utilisateur aux groupes (facultatif). Choisissez Modifier à chaque étape pour apporter des modifications. Après avoir confirmé que les informations correctes sont spécifiées pour les deux étapes, choisissez Ajouter un utilisateur.

Ajouter des groupes

Utilisez la procédure suivante pour ajouter des groupes à votre répertoire Identity Center à l'aide de la console IAM Identity Center. Vous pouvez également appeler l'opération AWS API CreateGrouppour ajouter des groupes.

Pour ajouter un groupe

1. Ouvrez la console IAM Identity Center.
2. Choisissez Groupes.
3. Choisissez Créer un groupe.
4. Entrez un nom et une description du groupe (facultatif). La description doit fournir des détails sur les autorisations qui ont été ou seront attribuées au groupe. Sous Ajouter des utilisateurs au groupe (facultatif), recherchez les utilisateurs que vous souhaitez ajouter en tant que membres. Activez ensuite la case à cocher en regard de chacun d'entre eux.
5. Choisissez Créer un groupe.

Après avoir ajouté ce groupe à votre répertoire Identity Center, vous pouvez lui attribuer un accès par authentification unique. Pour plus d'informations, consultez Attribuer un accès utilisateur à Comptes AWS.

Ajouter des utilisateurs à des groupes

Utilisez la procédure suivante pour ajouter des utilisateurs en tant que membres d'un groupe que vous avez créé précédemment dans votre répertoire Identity Center à l'aide de la console IAM Identity Center. Vous pouvez également appeler l'opération AWS API CreateGroupMembershippour ajouter un utilisateur en tant que membre d'un groupe.

Pour ajouter un utilisateur en tant que membre d'un groupe

1. Ouvrez la console IAM Identity Center.
2. Choisissez Groupes.

3. Choisissez le nom du groupe que vous souhaitez mettre à jour.
4. Sur la page des détails du groupe, sous Utilisateurs de ce groupe, choisissez Ajouter des utilisateurs au groupe.
5. Sur la page Ajouter des utilisateurs au groupe, sous Autres utilisateurs, recherchez les utilisateurs que vous souhaitez ajouter en tant que membres. Cochez ensuite la case à côté de chacun d'eux.
6. Sélectionnez Ajouter des utilisateurs.

Supprimer des groupes dans IAM Identity Center

Lorsque vous supprimez un groupe dans le répertoire de votre IAM Identity Center, tous les utilisateurs membres de ce groupe sont privés de l'accès à ces derniers Comptes AWS et de leurs applications. Une fois qu'un groupe est supprimé, il ne peut pas être annulé. Utilisez la procédure suivante pour supprimer un groupe dans votre répertoire Identity Center à l'aide de la console IAM Identity Center.

Pour supprimer un groupe dans IAM Identity Center

> **Important**
>
> Les instructions de cette page s'appliquent à AWS IAM Identity Center. Ils ne s'appliquent pas à AWS Identity and Access Management(IAM). Les utilisateurs, les groupes et les informations d'identification utilisateur d'IAM Identity Center sont différents des informations d'identification des utilisateurs, des groupes et des utilisateurs IAM. Si vous recherchez des instructions sur la suppression de groupes dans IAM, consultez la section Suppression d'un groupe d'utilisateurs IAM dans le guide de l'AWS Identity and Access Management utilisateur.

1. Ouvrez la console IAM Identity Center.
2. Choisissez Groupes.
3. Vous pouvez supprimer un groupe de deux manières :
   - Sur la page Groupes, vous pouvez sélectionner plusieurs groupes à supprimer. Sélectionnez le nom du groupe que vous souhaitez supprimer, puis choisissez Supprimer le groupe.
   - Choisissez le nom du groupe que vous souhaitez supprimer. Sur la page des détails du groupe, choisissez Supprimer le groupe.

4. Il vous sera peut-être demandé de confirmer votre intention de supprimer le groupe.

   - Si vous supprimez plusieurs groupes à la fois, confirmez votre intention **`Delete`** en saisissant du texte dans la boîte de dialogue Supprimer le groupe.
   - Si vous supprimez un seul groupe contenant des utilisateurs, confirmez votre intention en saisissant le nom du groupe que vous souhaitez supprimer dans la boîte de dialogue Supprimer le groupe.

5. Choisissez Supprimer un groupe. Si vous avez sélectionné plusieurs groupes à supprimer, choisissez Supprimer le nombre de groupes.

Supprimer des utilisateurs dans IAM Identity Center

Lorsque vous supprimez un utilisateur dans le répertoire de votre IAM Identity Center, il supprime son accès aux applications Comptes AWS et à ses applications. Une fois qu'un utilisateur est supprimé, il ne peut pas être annulé. Utilisez la procédure suivante pour supprimer un utilisateur de votre répertoire Identity Center à l'aide de la console IAM Identity Center.

> **Note**
>
> Lorsque vous désactivez l'accès d'un utilisateur ou que vous supprimez un utilisateur dans IAM Identity Center, cet utilisateur est immédiatement empêché de se connecter au portail d' AWS accès et ne pourra pas créer de nouvelles sessions de connexion. Pour plus d'informations, consultez Sessions d'authentification.

Pour supprimer un utilisateur dans IAM Identity Center

> **Important**
>
> Les instructions de cette page s'appliquent à AWS IAM Identity Center. Ils ne s'appliquent pas à AWS Identity and Access Management(IAM). Les utilisateurs, les groupes et les informations d'identification utilisateur d'IAM Identity Center sont différents des informations d'identification des utilisateurs, des groupes et des utilisateurs IAM. Si vous recherchez des instructions sur la suppression d'utilisateurs dans IAM, consultez la section Suppression d'un utilisateur IAM dans le guide de l'AWS Identity and Access Management utilisateur.

1. Ouvrez la console IAM Identity Center.

2. Choisissez Utilisateurs.
3. Vous pouvez supprimer un utilisateur de deux manières :
   - Sur la page Utilisateurs, vous pouvez sélectionner plusieurs utilisateurs à supprimer. Sélectionnez le nom d'utilisateur que vous souhaitez supprimer, puis choisissez Supprimer les utilisateurs.
   - Choisissez le nom d'utilisateur que vous souhaitez supprimer. Sur la page des informations de l'utilisateur, choisissez Supprimer l'utilisateur.
4. Si vous supprimez plusieurs utilisateurs à la fois, confirmez votre intention **`Delete`** en saisissant du texte dans la boîte de dialogue Supprimer un utilisateur.
5. Choisissez Delete user (Supprimer l'utilisateur). Si vous avez sélectionné plusieurs utilisateurs à supprimer, choisissez Supprimer le nombre d'utilisateurs.

Désactiver l'accès des utilisateurs dans IAM Identity Center

Lorsque vous désactivez l'accès des utilisateurs dans votre annuaire IAM Identity Center, vous ne pouvez pas modifier leurs informations d'utilisateur, réinitialiser leur mot de passe, ajouter l'utilisateur à un groupe ou consulter son appartenance à un groupe. Utilisez la procédure suivante pour désactiver l'accès des utilisateurs dans votre répertoire Identity Center à l'aide de la console IAM Identity Center.

> **Note**
>
> Lorsque vous désactivez l'accès d'un utilisateur ou que vous supprimez un utilisateur dans IAM Identity Center, cet utilisateur est immédiatement empêché de se connecter au portail d' AWS accès et ne pourra pas créer de nouvelles sessions de connexion. Pour plus d'informations, consultez Sessions d'authentification.

Pour désactiver l'accès des utilisateurs dans IAM Identity Center

1. Ouvrez la console IAM Identity Center.

> **Important**
>
> Les instructions de cette page s'appliquent à AWS IAM Identity Center. Ils ne s'appliquent pas à AWS Identity and Access Management(IAM). Les utilisateurs, les

groupes et les informations d'identification utilisateur d'IAM Identity Center sont différents des informations d'identification des utilisateurs, des groupes et des utilisateurs IAM. Si vous recherchez des instructions sur la désactivation des utilisateurs dans IAM, consultez la section Gestion des utilisateurs IAM dans le guide de l'AWS Identity and Access Management utilisateur.

2. Choisissez Utilisateurs.
3. Sélectionnez le nom d'utilisateur de l'utilisateur dont vous souhaitez désactiver l'accès.
4. Sous le nom d'utilisateur de l'utilisateur dont vous souhaitez désactiver l'accès, dans la section Informations générales, choisissez Désactiver l'accès utilisateur.
5. Dans la boîte de dialogue Désactiver l'accès utilisateur, choisissez Désactiver l'accès utilisateur.

Modifier les propriétés de l'utilisateur

Utilisez la procédure suivante pour modifier les propriétés d'un utilisateur dans votre répertoire Identity Center à l'aide de la console IAM Identity Center. Vous pouvez également appeler l'opération AWS API UpdateUserpour mettre à jour les propriétés de l'utilisateur.

Pour modifier les propriétés de l'utilisateur dans IAM Identity Center

1. Ouvrez la console IAM Identity Center.
2. Choisissez Utilisateurs.
3. Choisissez l'utilisateur que vous souhaitez modifier.
4. Sur la page du profil utilisateur, à côté de Détails du profil, sélectionnez Modifier.
5. Sur la page Modifier les détails du profil, mettez à jour les propriétés selon vos besoins. Ensuite, choisissez Save changes (Enregistrer les modifications).

> **Note**
>
> (Facultatif) Vous pouvez modifier des attributs supplémentaires tels que le numéro d'employé et l'identifiant immuable Office 365 pour aider à mapper l'identité de l'utilisateur dans IAM Identity Center avec certaines applications professionnelles que les utilisateurs doivent utiliser.

> **Note**
>
> L'attribut Adresse e-mail est un champ modifiable et la valeur que vous fournissez doit être unique.

Réinitialisation du mot de passe utilisateur IAM Identity Center pour un utilisateur final

Cette procédure est destinée aux administrateurs qui doivent réinitialiser le mot de passe d'un utilisateur dans votre répertoire IAM Identity Center. Vous allez utiliser la console IAM Identity Center pour réinitialiser les mots de passe.

Considérations relatives aux fournisseurs d'identité et aux types d'utilisateurs

- MicrosoftActive Directory ou fournisseur externe : si vous connectez IAM Identity Center à Microsoft Active Directory ou à un fournisseur externe, les réinitialisations du mot de passe utilisateur doivent être effectuées depuis Active Directory ou depuis le fournisseur externe. Cela signifie que les mots de passe de ces utilisateurs ne peuvent pas être réinitialisés depuis la console IAM Identity Center.
- Utilisateurs du répertoire IAM Identity Center : si vous êtes un utilisateur d'IAM Identity Center, vous pouvez réinitialiser votre propre mot de passe IAM Identity Center, voir. Réinitialisation de votre mot de passe utilisateur IAM Identity Center

Pour réinitialiser le mot de passe d'un utilisateur final d'IAM Identity Center

> **Important**
>
> Les instructions de cette page s'appliquent à AWS IAM Identity Center. Ils ne s'appliquent pas à AWS Identity and Access Management(IAM). Les utilisateurs, les groupes et les informations d'identification utilisateur d'IAM Identity Center sont différents des informations d'identification des utilisateurs, des groupes et des utilisateurs IAM. Si vous recherchez des instructions sur la modification des mots de passe des utilisateurs IAM, consultez la section Gestion des mots de passe des utilisateurs IAM dans le guide de l'AWS Identity and Access Management utilisateur.

1. Ouvrez la console IAM Identity Center.
2. Choisissez Utilisateurs.
3. Sélectionnez le nom d'utilisateur de l'utilisateur dont vous souhaitez réinitialiser le mot de passe.
4. Sur la page des informations de l'utilisateur, choisissez Réinitialiser le mot de passe.
5. Dans la boîte de dialogue Réinitialiser le mot de passe, sélectionnez l'une des options suivantes, puis choisissez Réinitialiser le mot de passe :

   a. Envoyez un e-mail à l'utilisateur avec des instructions pour réinitialiser le mot de passe — Cette option envoie automatiquement à l'utilisateur une adresse e-mail provenant d'Amazon Web Services qui lui explique comment réinitialiser son mot de passe.

   > **Warning**
   >
   > Pour des raisons de sécurité, vérifiez que l'adresse e-mail de cet utilisateur est correcte avant de sélectionner cette option. Si cet e-mail de réinitialisation du mot de passe devait être envoyé à une adresse e-mail incorrecte ou mal configurée, un destinataire malveillant pourrait l'utiliser pour obtenir un accès non autorisé à votre AWS environnement.

   b. Générez un mot de passe à usage unique et partagez-le avec l'utilisateur — Cette option vous fournit les détails du mot de passe que vous pouvez envoyer manuellement à l'utilisateur à partir de votre adresse e-mail.

Envoyer un e-mail OTP pour les utilisateurs créés à partir de l'API

Lorsque vous créez des utilisateurs à l'aide de l'opération CreateUserAPI, ils n'ont pas de mot de passe. Vous pouvez modifier cela en choisissant d'envoyer aux utilisateurs un mot de passe à usage unique (OTP) par e-mail lors de leur création avec l'API. Les utilisateurs reçoivent l'e-mail OTP lorsqu'ils tentent de se connecter pour la première fois. Après avoir reçu l'e-mail OTP, lorsqu'un utilisateur se connecte, il doit définir un nouveau mot de passe. Si vous n'activez pas ce paramètre, vous devez générer et partager l'OTP avec les utilisateurs que vous créez à l'aide de l'CreateUserAPI.

Pour envoyer un e-mail OTP aux utilisateurs créés avec l'API CreateUser

1. Ouvrez la console IAM Identity Center.
2. Sélectionnez Settings (Paramètres).

3. Sur la page Paramètres, choisissez l'onglet Authentification.
4. Dans la section Authentification standard, choisissez Configurer.
5. Une boîte de dialogue apparaît. Cochez la case à côté de Envoyer un e-mail OTP. Ensuite, choisissez Enregistrer. Le statut passe de Désactivé à Activé.

Exigences relatives aux mots de passe lors de la gestion des identités dans IAM Identity Center

> **Note**
>
> Ces exigences s'appliquent uniquement aux utilisateurs créés dans le répertoire Identity Center. Si vous avez configuré une source d'identité autre qu'IAM Identity Center pour l'authentification, telle qu'un fournisseur Active Directoryd'identité externe, les politiques de mot de passe pour vos utilisateurs sont définies et appliquées dans ces systèmes, et non dans IAM Identity Center. Si votre source d'identité l'est AWS Managed Microsoft AD, consultez Gérer les politiques de mot de passe AWS Managed Microsoft AD pour plus d'informations.

Lorsque vous utilisez IAM Identity Center comme source d'identité, les utilisateurs doivent respecter les exigences de mot de passe suivantes pour définir ou modifier leur mot de passe :

- Les mots de passe distinguent majuscules et minuscules.
- Les mots de passe doivent comporter entre 8 et 64 caractères.
- Les mots de passe doivent contenir au moins un caractère appartenant à chacune des quatre catégories suivantes :
  - Lettres minuscules (a-z)
  - Lettres majuscules (A-Z)
  - Chiffres (0-9)
  - Caractères non alphanumériques (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
- Les trois derniers mots de passe ne peuvent pas être réutilisés.
- Les mots de passe connus du public grâce à un ensemble de données divulgué par un tiers ne peuvent pas être utilisés.

Se connecter à un Microsoft AD annuaire

Avec AWS IAM Identity Center, vous pouvez connecter un annuaire autogéré dans Active Directory (AD) ou un annuaire dans en AWS Managed Microsoft AD utilisant AWS Directory Service. Ce répertoire Microsoft AD définit le pool d'identités que les administrateurs peuvent extraire lorsqu'ils utilisent la console IAM Identity Center pour attribuer un accès par authentification unique. Après avoir connecté votre annuaire d'entreprise à IAM Identity Center, vous pouvez autoriser vos utilisateurs ou groupes AD à accéder aux applications Comptes AWS, ou aux deux.

AWS Directory Service vous aide à configurer et à gérer un AWS Managed Microsoft AD annuaire autonome hébergé dans le AWS Cloud. Vous pouvez également l'utiliser AWS Directory Service pour connecter vos AWS ressources à un AD autogéré existant. Pour que AWS Directory Service la configuration fonctionne avec votre AD autogéré, vous devez d'abord établir des relations de confiance afin d'étendre l'authentification au cloud.

IAM Identity Center utilise la connexion fournie par AWS Directory Service pour effectuer une authentification directe sur l'instance AD source. Lorsque vous l'utilisez AWS Managed Microsoft AD comme source d'identité, IAM Identity Center peut travailler avec des utilisateurs depuis AWS Managed Microsoft AD ou vers n'importe quel domaine connecté via un AD Trust. Si vous souhaitez localiser vos utilisateurs dans quatre domaines ou plus, les utilisateurs doivent utiliser la `DOMAIN\user` syntaxe comme nom d'utilisateur lorsqu'ils se connectent à IAM Identity Center.

> **Remarques**
>
> - Comme étape préalable, assurez-vous que votre AD Connector ou votre répertoire dans AWS Managed Microsoft AD in AWS Directory Service se trouve dans votre compte AWS Organizations de gestion. Pour de plus amples informations, veuillez consulter Confirmez vos sources d'identité dans IAM Identity Center.
> - IAM Identity Center ne prend pas en charge Simple AD basé sur SAMBA 4 en tant qu'annuaire connecté.

Considérations relatives à l'utilisation d'Active Directory

Si vous souhaitez utiliser Active Directory comme source d'identité, votre configuration doit répondre aux conditions préalables suivantes :

- Si vous utilisez AWS Managed Microsoft AD, vous devez activer IAM Identity Center au même Région AWS endroit où votre AWS Managed Microsoft AD annuaire est configuré. IAM Identity Center stocke les données d'attribution dans la même région que le répertoire. Pour administrer IAM Identity Center, vous devrez peut-être passer à la région dans laquelle IAM Identity Center est configuré. Notez également que le portail AWS d'accès utilise la même URL d'accès que votre annuaire.
- Utilisez un Active Directory résidant dans le compte de gestion :

  Un AD Connector ou un AWS Managed Microsoft AD annuaire AD Connector existant doit être configuré dans AWS Directory Servicevotre compte AWS Organizations de gestion. Vous ne pouvez connecter qu'un seul répertoire AD Connector ou un seul annuaire AWS Managed Microsoft AD à la fois. Si vous devez prendre en charge plusieurs domaines ou forêts, utilisez AWS Managed Microsoft AD. Pour plus d'informations, consultez :

  - Connecter un annuaire AWS Managed Microsoft AD à IAM Identity Center
  - Connectez un annuaire autogéré dans Active Directory à IAM Identity Center
- Utilisez un Active Directory résidant dans le compte administrateur délégué :

  Si vous envisagez d'activer l'administrateur délégué d'IAM Identity Center et d'utiliser Active Directory comme source d'identité IAM Identity Center, vous pouvez utiliser un connecteur AD Connector ou un AWS Managed Microsoft AD annuaire existant configuré dans AWS Directory résidant dans le compte d'administrateur délégué.

  Si vous décidez de remplacer la source d'identité d'IAM Identity Center par une autre source par Active Directory, ou de passer d'Active Directory à une autre source, le répertoire doit résider (appartenir à) le compte membre administrateur délégué d'IAM Identity Center, s'il en existe un ; sinon, il doit figurer dans le compte de gestion.

Connectez Active Directory et spécifiez un utilisateur

Si vous utilisez déjà Active Directory, les rubriques suivantes vous aideront à préparer la connexion de votre annuaire à IAM Identity Center.

Vous pouvez connecter un AWS Managed Microsoft AD annuaire ou un annuaire autogéré dans Active Directory avec IAM Identity Center. Si vous envisagez de connecter un AWS Managed Microsoft AD annuaire ou un annuaire autogéré dans Active Directory, assurez-vous que votre configuration Active Directory répond aux conditions requises dans. Confirmez vos sources d'identité dans IAM Identity Center

> **Note**
>
> Pour des raisons de sécurité, nous vous recommandons vivement d'activer l'authentification multifactorielle. Si vous envisagez de connecter un AWS Managed Microsoft AD annuaire ou un annuaire autogéré dans Active Directory et que vous n'utilisez pas RADIUS MFA AWS Directory Serviceavec, activez l'authentification MFA dans IAM Identity Center.

AWS Managed Microsoft AD

1. Consultez les directives dansSe connecter à un Microsoft AD annuaire.
2. Suivez les étapes de Connecter un annuaire AWS Managed Microsoft AD à IAM Identity Center.
3. Configurez Active Directory pour synchroniser l'utilisateur auquel vous souhaitez accorder des autorisations administratives dans IAM Identity Center. Pour de plus amples informations, veuillez consulter Synchroniser un utilisateur administratif dans IAM Identity Center.

Annuaire autogéré dans Active Directory

1. Consultez les directives dansSe connecter à un Microsoft AD annuaire.
2. Suivez les étapes de Connectez un annuaire autogéré dans Active Directory à IAM Identity Center.
3. Configurez Active Directory pour synchroniser l'utilisateur auquel vous souhaitez accorder des autorisations administratives dans IAM Identity Center. Pour de plus amples informations, veuillez consulter Synchroniser un utilisateur administratif dans IAM Identity Center.

IdP externe

1. Consultez les directives dansConnectez-vous à un fournisseur d'identité externe.
2. Suivez les étapes de Comment se connecter à un fournisseur d'identité externe.
3. Configurez votre IdP pour connecter les utilisateurs à IAM Identity Center.

> **Note**
>
> Avant de configurer le provisionnement automatique par groupe de toutes les identités de votre personnel, depuis votre IdP vers IAM Identity Center, nous vous recommandons de

synchroniser l'utilisateur auquel vous souhaitez accorder des autorisations administratives dans IAM Identity Center.

Synchroniser un utilisateur administratif dans IAM Identity Center

Après avoir connecté votre annuaire à IAM Identity Center, vous pouvez spécifier un utilisateur auquel vous souhaitez accorder des autorisations administratives, puis synchroniser cet utilisateur depuis votre annuaire avec IAM Identity Center.

1. Ouvrez la console IAM Identity Center.
2. Sélectionnez Settings (Paramètres).
3. Sur la page Paramètres, choisissez l'onglet Source d'identité, sélectionnez Actions, puis sélectionnez Gérer la synchronisation.
4. Sur la page Gérer la synchronisation, choisissez l'onglet Utilisateurs, puis sélectionnez Ajouter des utilisateurs et des groupes.
5. Dans l'onglet Utilisateurs, sous Utilisateur, entrez le nom d'utilisateur exact et choisissez Ajouter.
6. Sous Utilisateurs et groupes ajoutés, procédez comme suit :
    a. Vérifiez que l'utilisateur auquel vous souhaitez accorder des autorisations administratives est spécifié.
    b. Cochez la case située à gauche du nom d'utilisateur.
    c. Sélectionnez Envoyer.
7. Sur la page Gérer la synchronisation, l'utilisateur que vous avez spécifié apparaît dans la liste Utilisateurs synchronisés.
8. Dans le panneau de navigation, choisissez utilisateurs.
9. Sur la page Utilisateurs, l'utilisateur que vous avez spécifié peut mettre un certain temps à apparaître dans la liste. Cliquez sur l'icône d'actualisation pour mettre à jour la liste des utilisateurs.

À ce stade, votre utilisateur n'a pas accès au compte de gestion. Vous allez configurer l'accès administratif à ce compte en créant un ensemble d'autorisations administratives et en affectant l'utilisateur à cet ensemble d'autorisations. Pour de plus amples informations, veuillez consulter Crée un jeu d'autorisations..

Provisionnement lorsque les utilisateurs proviennent d'Active Directory

IAM Identity Center utilise la connexion fournie par le AWS Directory Service pour synchroniser les informations relatives aux utilisateurs, aux groupes et aux membres entre votre répertoire source dans Active Directory et le magasin d'identités IAM Identity Center. Aucune information de mot de passe n'est synchronisée avec IAM Identity Center, car l'authentification des utilisateurs s'effectue directement depuis le répertoire source dans Active Directory. Ces données d'identité sont utilisées par les applications pour faciliter les scénarios de recherche, d'autorisation et de collaboration intégrés à l'application sans renvoyer l'activité LDAP au répertoire source dans Active Directory.

Pour plus d'informations ci-dessus sur le provisionnement, consultezProvisionnement d'utilisateurs et de groupes.

Rubriques

- Connecter un annuaire AWS Managed Microsoft AD à IAM Identity Center
- Connectez un annuaire autogéré dans Active Directory à IAM Identity Center
- Mappages d'attributs pour le répertoire AWS Managed Microsoft AD
- Provisionner des utilisateurs et des groupes à partir d'Active Directory

Connecter un annuaire AWS Managed Microsoft AD à IAM Identity Center

Utilisez la procédure suivante pour connecter un répertoire géré par AWS Directory Service à IAM Identity Center. AWS Managed Microsoft AD

Pour vous connecter AWS Managed Microsoft AD à IAM Identity Center

1. Ouvrez la console IAM Identity Center.

   > **Note**
   >
   > Assurez-vous que la console IAM Identity Center utilise l'une des régions dans lesquelles se trouve votre AWS Managed Microsoft AD répertoire avant de passer à l'étape suivante.

2. Sélectionnez Settings (Paramètres).
3. Sur la page Paramètres, choisissez l'onglet Source d'identité, puis Actions > Modifier la source d'identité.

4. Sous Choisir la source d'identité, sélectionnez Active Directory, puis Next.
5. Sous Connect Active Directory, choisissez un répertoire dans AWS Managed Microsoft AD la liste, puis choisissez Next.
6. Sous Confirmer la modification, passez en revue les informations et lorsque vous êtes prêt, tapez ACCEPT, puis choisissez Modifier la source d'identité.

> **Important**
>
> Pour spécifier un utilisateur dans Active Directory en tant qu'utilisateur administratif dans IAM Identity Center, vous devez d'abord synchroniser l'utilisateur auquel vous souhaitez accorder des autorisations administratives depuis Active Directory vers IAM Identity Center. Pour ce faire, suivez les étapes de Synchroniser un utilisateur administratif dans IAM Identity Center.

Connectez un annuaire autogéré dans Active Directory à IAM Identity Center

Les utilisateurs de votre annuaire autogéré dans Active Directory (AD) peuvent également accéder par authentification unique au portail d'accès Comptes AWS et aux applications qui s' AWS y trouvent. Pour configurer l'accès à authentification unique pour ces utilisateurs, vous pouvez effectuer l'une des opérations suivantes :

- Création d'une relation de confiance bidirectionnelle : lorsque des relations de confiance bidirectionnelles sont créées entre AWS Managed Microsoft AD et un annuaire autogéré dans AD, les utilisateurs de votre annuaire autogéré dans AD peuvent se connecter avec leurs informations d'identification d'entreprise à divers AWS services et applications métier. Les approbations unidirectionnelles ne fonctionnent pas avec IAM Identity Center.

  AWS IAM Identity Center nécessite une confiance bidirectionnelle afin d'être autorisé à lire les informations relatives aux utilisateurs et aux groupes de votre domaine afin de synchroniser les métadonnées des utilisateurs et des groupes. IAM Identity Center utilise ces métadonnées pour attribuer l'accès à des ensembles d'autorisations ou à des applications. Les métadonnées des utilisateurs et des groupes sont également utilisées par les applications à des fins de collaboration, par exemple lorsque vous partagez un tableau de bord avec un autre utilisateur ou un autre groupe. La confiance accordée par AWS Directory Service Microsoft Active Directory à votre domaine permet à IAM Identity Center de faire confiance à votre domaine pour l'authentification.

La confiance dans le sens opposé accorde des AWS autorisations pour lire les métadonnées des utilisateurs et des groupes.

Pour plus d'informations sur la configuration d'une confiance bidirectionnelle, voir Quand créer une relation de confiance dans le Guide d'AWS Directory Service administration.

- Création d'un AD Connector — AD Connector est une passerelle d'annuaire qui peut rediriger les demandes d'annuaire vers votre AD autogéré sans mettre en cache aucune information dans le cloud. Pour plus d'informations, voir Connect to a Directory dans le GuideAWS Directory Service d'administration.

> **Note**
>
> Si vous connectez IAM Identity Center à un annuaire AD Connector, toute future réinitialisation du mot de passe utilisateur devra être effectuée depuis AD. Cela signifie que les utilisateurs ne pourront pas réinitialiser leur mot de passe depuis le portail AWS d'accès.
> Si vous utilisez AD Connector pour connecter votre service de domaine Active Directory à IAM Identity Center, IAM Identity Center n'a accès qu'aux utilisateurs et aux groupes du domaine unique auquel AD Connector est attaché. Si vous devez prendre en charge plusieurs domaines ou forêts, utilisez AWS Directory Service Microsoft Active Directory.

> **Note**
>
> IAM Identity Center ne fonctionne pas avec les annuaires Simple AD basés sur Samba4.

Mappages d'attributs pour le répertoire AWS Managed Microsoft AD

Les mappages d'attributs sont utilisés pour mapper les types d'attributs qui existent dans IAM Identity Center avec des attributs similaires dans un AWS Managed Microsoft AD annuaire. IAM Identity Center extrait les attributs utilisateur de votre répertoire Microsoft AD et les associe aux attributs utilisateur IAM Identity Center. Ces mappages d'attributs utilisateur IAM Identity Center sont également utilisés pour générer des assertions SAML 2.0 pour vos applications. Chaque application détermine la liste des attributs SAML 2.0 dont elle a besoin pour une authentification unique réussie.

IAM Identity Center préremplit un ensemble d'attributs pour vous sous l'onglet Mappages d'attributs situé sur la page de configuration de votre application. IAM Identity Center utilise ces attributs

utilisateur pour remplir les assertions SAML (sous forme d'attributs SAML) qui sont envoyées à l'application. Ces attributs utilisateur sont ensuite extraits de votre annuaire Microsoft AD. Pour de plus amples informations, veuillez consulter Associez les attributs de votre application aux attributs d'IAM Identity Center.

IAM Identity Center gère également un ensemble d'attributs pour vous dans la section Mappages d'attributs de la page de configuration de votre annuaire. Pour de plus amples informations, veuillez consulter Associez les attributs d'IAM Identity Center aux attributs de votre annuaire AWS Managed Microsoft AD.

Attributs de répertoire supportés

Le tableau suivant répertorie tous les attributs d' AWS Managed Microsoft AD annuaire pris en charge et pouvant être mappés aux attributs utilisateur dans IAM Identity Center.

Attributs pris en charge dans votre annuaire Microsoft AD
`${dir:email}`
`${dir:displayname}`
`${dir:distinguishedName}`
`${dir:firstname}`
`${dir:guid}`
`${dir:initials}`
`${dir:lastname}`
`${dir:proxyAddresses}`
`${dir:proxyAddresses:smtp}`
`${dir:proxyAddresses:SMTP}`
`${dir:windowsUpn}`

Vous pouvez spécifier n'importe quelle combinaison d'attributs d'annuaire Microsoft AD pris en charge à mapper à un seul attribut mutable dans IAM Identity Center. Par exemple, vous pouvez choisir l'`subject`attribut sous l'attribut Utilisateur dans la colonne IAM Identity Center. Mappez-le ensuite à l'un `${dir:displayname}` `${dir:lastname}${dir:firstname }` ou l'autre des attributs pris en charge ou à une combinaison arbitraire d'attributs pris en charge. Pour obtenir la liste des mappages par défaut pour les attributs utilisateur dans IAM Identity Center, consultez. Mappages par défaut

> **Warning**
>
> Certains attributs d'IAM Identity Center ne peuvent pas être modifiés car ils sont immuables et mappés par défaut à des attributs d'annuaire Microsoft AD spécifiques.
> Par exemple, « nom d'utilisateur » est un attribut obligatoire dans IAM Identity Center. Si vous associez « nom d'utilisateur » à un attribut d'annuaire AD avec une valeur vide, IAM Identity Center considérera cette `windowsUpn` valeur comme valeur par défaut pour « nom d'utilisateur ». Si vous souhaitez modifier le mappage d'attributs pour « nom d'utilisateur » par rapport à votre mappage actuel, vérifiez que les flux IAM Identity Center dépendants du « nom d'utilisateur » continueront de fonctionner comme prévu, avant d'effectuer la modification.

Si vous utilisez les actions ListUsersou ListGroupsAPI ou les commandes list-usersset list-groups AWS CLI pour attribuer aux utilisateurs et aux groupes l'accès aux Comptes AWS applications, vous devez spécifier la valeur pour en `AttributeValue` tant que FQDN. Cette valeur doit être au format suivant : user@example.com. Dans l'exemple suivant, `AttributeValue` est défini sur`janedoe@example.com`.

```
aws identitystore list-users --identity-store-id d-12345a678b --filters
 AttributePath=UserName,AttributeValue=janedoe@example.com
```

Attributs IAM Identity Center pris en charge

Le tableau suivant répertorie tous les attributs IAM Identity Center pris en charge et pouvant être mappés aux attributs utilisateur de votre AWS Managed Microsoft AD annuaire. Après avoir configuré les mappages d'attributs de votre application, vous pouvez utiliser ces mêmes attributs IAM Identity Center pour les mapper aux attributs réels utilisés par cette application.

Attributs pris en charge dans IAM Identity Center
`${user:AD_GUID}`
`${user:email}`
`${user:familyName}`
`${user:givenName}`
`${user:middleName}`
`${user:name}`
`${user:preferredUsername}`
`${user:subject}`

Attributs du fournisseur d'identité externe pris en charge

Le tableau suivant répertorie tous les attributs du fournisseur d'identité externe (IdP) pris en charge et pouvant être mappés aux attributs que vous pouvez utiliser lors de la configuration Attributs pour le contrôle d'accès dans IAM Identity Center. Lorsque vous utilisez des assertions SAML, vous pouvez utiliser les attributs pris en charge par votre IdP.

Attributs pris en charge dans votre IdP
`${path:userName}`
`${path:name.familyName}`
`${path:name.givenName}`
`${path:displayName}`
`${path:nickName}`
`${path:emails[primary eq true].value}`
`${path:addresses[type eq "work"].streetAddress}`

Attributs pris en charge dans votre IdP
`${path:addresses[type eq "work"].locality}`
`${path:addresses[type eq "work"].region}`
`${path:addresses[type eq "work"].postalCode}`
`${path:addresses[type eq "work"].country}`
`${path:addresses[type eq "work"].formatted}`
`${path:phoneNumbers[type eq "work"].value}`
`${path:userType}`
`${path:title}`
`${path:locale}`
`${path:timezone}`
`${path:enterprise.employeeNumber}`
`${path:enterprise.costCenter}`
`${path:enterprise.organization}`
`${path:enterprise.division}`
`${path:enterprise.department}`
`${path:enterprise.manager.value}`

Mappages par défaut

Le tableau suivant répertorie les mappages par défaut des attributs utilisateur dans IAM Identity Center avec les attributs utilisateur de votre AWS Managed Microsoft AD annuaire. IAM Identity Center prend uniquement en charge la liste des attributs de l'attribut Utilisateur dans la colonne IAM Identity Center.

> **Note**
>
> Si vous n'avez aucune attribution pour vos utilisateurs et groupes dans IAM Identity Center lorsque vous activez la synchronisation AD configurable, les mappages par défaut du tableau suivant sont utilisés. Pour plus d'informations sur la personnalisation de ces mappages, consultezConfigurez les mappages d'attributs pour votre synchronisation.

Attribut utilisateur dans IAM Identity Center	Mappé à cet attribut dans votre annuaire Microsoft AD
`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}`

* L'attribut e-mail dans IAM Identity Center doit être unique dans l'annuaire. Dans le cas contraire, le processus de connexion au JIT risque d'échouer.

Vous pouvez modifier les mappages par défaut ou ajouter d'autres attributs à l'assertion SAML 2.0 en fonction de vos besoins. Supposons, par exemple, que votre application nécessite l'adresse e-mail de l'utilisateur dans l'attribut `User.Email` SAML 2.0. Supposons également que les adresses e-mail soient stockées dans l'`windowsUpn`attribut de votre répertoire Microsoft AD. Pour réaliser ce mappage, vous devez apporter des modifications aux deux emplacements suivants dans la console IAM Identity Center :

1. Sur la page Directory (Annuaire), sous la section Attribute mappings (Mappages d'attributs), vous devez mapper l'attribut utilisateur **`email`** à l'attribut **`${dir:windowsUpn}`** (dans la colonne Maps to this attribute in your directory (Mappé à cet attribut dans votre annuaire)).
2. Sur la page Applications, sélectionnez l'application dans le tableau. Choisissez l'onglet Mappages d'attributs. Mappez ensuite l'`User.Email`attribut à l'**`${user:email}`**attribut (dans la colonne Mappé à cette valeur de chaîne ou à cet attribut utilisateur dans le centre d'identité IAM).

Notez que vous devez fournir chaque attribut de répertoire sous la forme $ {dir :**`AttributeName`**}. Par exemple, l'attribut `firstname` dans votre annuaire Microsoft AD devient `${dir:firstname}`. Il importe qu'une valeur réelle soit attribuée à chaque attribut d'annuaire. Les attributs sans valeur après `${dir:` entraînent des problèmes de connexion utilisateur.

Associez les attributs d'IAM Identity Center aux attributs de votre annuaire AWS Managed Microsoft AD

Vous pouvez utiliser la procédure suivante pour spécifier comment vos attributs utilisateur dans IAM Identity Center doivent correspondre aux attributs correspondants dans votre annuaire Microsoft AD.

Pour mapper les attributs d'IAM Identity Center aux attributs de votre annuaire

1. Ouvrez la console IAM Identity Center.
2. Sélectionnez Settings (Paramètres).
3. Sur la page Paramètres, choisissez l'onglet Attributs pour le contrôle d'accès, puis sélectionnez Gérer les attributs.
4. Sur la page Gérer l'attribut pour le contrôle d'accès, recherchez l'attribut que vous souhaitez mapper dans IAM Identity Center, puis tapez une valeur dans la zone de texte. Par exemple, vous souhaiterez peut-être mapper l'attribut utilisateur IAM Identity Center **`email`**à l'attribut d'annuaire Microsoft AD. **`${dir:windowsUpn}`**
5. Sélectionnez Enregistrer les modifications.

Provisionner des utilisateurs et des groupes à partir d'Active Directory

IAM Identity Center propose les deux méthodes suivantes pour approvisionner des utilisateurs et des groupes à partir d'Active Directory.

- Synchronisation Active Directory (AD) configurable par IAM Identity Center (recommandée) — Cette méthode de synchronisation vous permet d'effectuer les opérations suivantes :

  - Contrôlez les limites des données en définissant explicitement les utilisateurs et les groupes dans Microsoft Active Directory qui sont automatiquement synchronisés dans IAM Identity Center. Vous pouvez ajouter des utilisateurs et des groupes ou supprimer des utilisateurs et des groupes pour modifier l'étendue de la synchronisation à tout moment.
  - Attribuez aux utilisateurs et aux groupes synchronisés un accès par authentification unique Comptes AWSou un accès aux applications. Les applications peuvent être des applications AWS gérées ou des applications gérées par le client.
  - Contrôlez le processus de synchronisation en interrompant et en reprenant la synchronisation selon les besoins. Cela vous permet de réguler la charge sur les systèmes de production.
- Synchronisation AD de IAM Identity Center : avec cette méthode de synchronisation, vous utilisez IAM Identity Center pour attribuer aux utilisateurs et aux groupes d'Active Directory l'accès à AWS des comptes et à des applications. Toutes les identités associées à des attributions sont automatiquement synchronisées dans IAM Identity Center.

Synchronisation AD configurable par IAM Identity Center

La synchronisation Active Directory (AD) configurable par IAM Identity Center vous permet de configurer explicitement les identités dans Microsoft Active Directory qui sont automatiquement synchronisées dans IAM Identity Center et de contrôler le processus de synchronisation.

Les rubriques suivantes fournissent des informations vous permettant de configurer et d'administrer une synchronisation AD configurable.

Rubriques

- Prérequis et considérations
- Comment fonctionne la synchronisation AD configurable
- Configuration et gestion de votre étendue de synchronisation

Prérequis et considérations

Avant d'utiliser la synchronisation AD configurable, tenez compte des conditions préalables et des considérations suivantes :

- Spécification des utilisateurs et des groupes à synchroniser dans Active Directory

  Avant de pouvoir utiliser IAM Identity Center pour attribuer à de nouveaux utilisateurs et groupes l'accès à Comptes AWS des applications AWS gérées ou à des applications gérées par le client,

vous devez spécifier les utilisateurs et les groupes à synchroniser dans Active Directory, puis les synchroniser dans IAM Identity Center.

- Synchronisation AD : lorsque vous attribuez des attributions à de nouveaux utilisateurs et groupes à l'aide de la console IAM Identity Center ou d'actions d'API d'attribution associées, IAM Identity Center recherche directement dans le contrôleur de domaine les utilisateurs ou groupes spécifiés, termine l'attribution, puis synchronise périodiquement les métadonnées de l'utilisateur ou du groupe dans IAM Identity Center.
- Synchronisation AD configurable : IAM Identity Center ne recherche pas directement les utilisateurs et les groupes dans votre contrôleur de domaine. Au lieu de cela, vous devez d'abord spécifier la liste des utilisateurs et des groupes à synchroniser. Vous pouvez configurer cette liste, également appelée étendue de synchronisation, de l'une des manières suivantes, selon que vous avez des utilisateurs et des groupes déjà synchronisés dans IAM Identity Center ou que vous avez de nouveaux utilisateurs et groupes que vous synchronisez pour la première fois à l'aide de la synchronisation AD configurable.
  - Utilisateurs et groupes existants : si certains de vos utilisateurs et groupes sont déjà synchronisés dans IAM Identity Center, l'étendue de synchronisation dans la synchronisation AD configurable est préremplie avec une liste de ces utilisateurs et groupes. Pour attribuer de nouveaux utilisateurs ou groupes, vous devez les ajouter spécifiquement à la zone de synchronisation. Pour de plus amples informations, veuillez consulter Ajoutez des utilisateurs et des groupes à votre zone de synchronisation.
  - Nouveaux utilisateurs et groupes : si vous souhaitez attribuer à de nouveaux utilisateurs et groupes l'accès aux Comptes AWS applications, vous devez spécifier les utilisateurs et les groupes à ajouter à l'étendue de synchronisation dans AD Sync configurable avant de pouvoir utiliser IAM Identity Center pour effectuer l'attribution. Pour de plus amples informations, veuillez consulter Ajoutez des utilisateurs et des groupes à votre zone de synchronisation.

- Attribuer des attributions à des groupes imbriqués dans Active Directory

  Les groupes membres d'autres groupes sont appelés groupes imbriqués (ou groupes d'enfants). Lorsque vous attribuez des attributions à un groupe dans Active Directory qui contient des groupes imbriqués, la manière dont les attributions sont appliquées varie selon que vous utilisez AD Sync ou AD Sync configurable.

  - Synchronisation AD : lorsque vous attribuez des attributions à un groupe dans Active Directory qui contient des groupes imbriqués, seuls les membres directs du groupe peuvent accéder au compte. Par exemple, si vous accordez l'accès au groupe A et que le groupe B est membre du

groupe A, seuls les membres directs du groupe A peuvent accéder au compte. Aucun membre du groupe B n'hérite de cet accès.

- Synchronisation AD configurable : l'utilisation de la synchronisation AD configurable pour attribuer des attributions à un groupe dans Active Directory contenant des groupes imbriqués peut augmenter le nombre d'utilisateurs ayant accès aux applications Comptes AWS ou à celles-ci. Dans ce cas, l'attribution s'applique à tous les utilisateurs, y compris ceux des groupes imbriqués. Par exemple, si vous accordez l'accès au groupe A et que le groupe B est membre du groupe A, les membres du groupe B héritent également de cet accès.

- Mise à jour des workflows automatisés

  Si vous avez des flux de travail automatisés qui utilisent les actions de l'API du magasin d'identités IAM Identity Center et les actions de l'API d'attribution d'IAM Identity Center pour attribuer aux nouveaux utilisateurs et groupes l'accès aux comptes et aux applications, et pour les synchroniser dans IAM Identity Center, vous devez ajuster ces flux de travail avant le 15 avril 2022 afin qu'ils fonctionnent comme prévu avec la synchronisation AD configurable. La synchronisation AD configurable modifie l'ordre dans lequel l'attribution et le provisionnement des utilisateurs et des groupes ont lieu, ainsi que la manière dont les requêtes sont effectuées.

  - Synchronisation AD : le processus d'attribution a lieu en premier. Vous attribuez aux utilisateurs Comptes AWS et aux groupes l'accès aux applications. Une fois que l'accès est attribué aux utilisateurs et aux groupes, ils sont automatiquement provisionnés (synchronisés dans IAM Identity Center). Si vous disposez d'un flux de travail automatisé, cela signifie que lorsque vous ajoutez un nouvel utilisateur à Active Directory, celui-ci peut interroger Active Directory pour l'utilisateur en utilisant l'action `ListUser` API du magasin d'identités, puis attribuer l'accès à l'utilisateur à l'aide des actions de l'API d'attribution IAM Identity Center. Comme l'utilisateur dispose d'une attribution, il est automatiquement approvisionné dans IAM Identity Center.
  - Synchronisation AD configurable : le provisionnement a lieu en premier et n'est pas effectué automatiquement. Au lieu de cela, vous devez d'abord ajouter explicitement des utilisateurs et des groupes au magasin d'identités en les ajoutant à votre étendue de synchronisation. Pour plus d'informations sur les étapes recommandées pour automatiser votre configuration de synchronisation pour une synchronisation AD configurable, consultezAutomatisez votre configuration de synchronisation pour une synchronisation AD configurable.

Comment fonctionne la synchronisation AD configurable

IAM Identity Center actualise les données d'identité basées sur la publicité dans le magasin d'identités en utilisant le processus suivant.

Création

Après avoir connecté votre annuaire autogéré dans Active Directory ou votre AWS Managed Microsoft AD annuaire géré par AWS Directory Service IAM Identity Center, vous pouvez configurer de manière explicite les utilisateurs et les groupes Active Directory que vous souhaitez synchroniser dans le magasin d'identités IAM Identity Center. Les identités que vous choisissez seront synchronisées toutes les trois heures environ dans le magasin d'identités IAM Identity Center. En fonction de la taille de votre répertoire, le processus de synchronisation peut prendre plus de temps.

Les groupes membres d'autres groupes (appelés groupes imbriqués ou groupes enfants) sont également enregistrés dans le magasin d'identités. Lorsque vous attribuez des attributions à un groupe dans Active Directory qui contient des groupes imbriqués, la manière dont les attributions sont appliquées varie selon que vous utilisez AD Sync ou AD Sync configurable. Pour de plus amples informations, veuillez consulter Making assignments to nested groups in Active Directory.

Vous ne pouvez attribuer l'accès à de nouveaux utilisateurs ou groupes qu'après leur synchronisation dans la banque d'identités IAM Identity Center.

Mettre à jour

Les données d'identité de la banque d'identités d'IAM Identity Center restent actualisées en lisant régulièrement les données du répertoire source dans Active Directory. IAM Identity Center synchronise les données de votre Active Directory toutes les heures selon un cycle de synchronisation par défaut. La synchronisation des données dans IAM Identity Center peut prendre entre 30 minutes et 2 heures, en fonction de la taille de votre Active Directory.

Les objets d'utilisateur et de groupe inclus dans la zone de synchronisation et leurs appartenances sont créés ou mis à jour dans IAM Identity Center pour être mappés aux objets correspondants dans le répertoire source d'Active Directory. Pour les attributs utilisateur, seul le sous-ensemble d'attributs répertorié dans la section Attributs pour le contrôle d'accès de la console IAM Identity Center est mis à jour dans IAM Identity Center. Un cycle de synchronisation peut être nécessaire pour que les mises à jour d'attributs que vous effectuez dans Active Directory soient répercutées dans IAM Identity Center.

Vous pouvez également mettre à jour le sous-ensemble d'utilisateurs et de groupes que vous synchronisez dans la banque d'identités IAM Identity Center. Vous pouvez choisir d'ajouter de nouveaux utilisateurs ou groupes à ce sous-ensemble ou de les supprimer. Toutes les identités que vous ajoutez sont synchronisées lors de la prochaine synchronisation planifiée. Les identités

que vous supprimez du sous-ensemble ne seront plus mises à jour dans la banque d'identités IAM Identity Center. Tout utilisateur qui n'est pas synchronisé pendant plus de 28 jours sera désactivé dans la banque d'identités IAM Identity Center. Les objets utilisateur correspondants seront automatiquement désactivés dans la banque d'identités IAM Identity Center lors du prochain cycle de synchronisation, sauf s'ils font partie d'un autre groupe qui fait toujours partie de la zone de synchronisation.

Suppression

Les utilisateurs et les groupes sont supprimés de la banque d'identités IAM Identity Center lorsque les objets d'utilisateur ou de groupe correspondants sont supprimés du répertoire source dans Active Directory. Vous pouvez également supprimer explicitement des objets utilisateur de la banque d'identités IAM Identity Center à l'aide de la console IAM Identity Center. Si vous utilisez la console IAM Identity Center, vous devez également supprimer les utilisateurs de la zone de synchronisation afin de vous assurer qu'ils ne seront pas resynchronisés dans IAM Identity Center lors du prochain cycle de synchronisation.

Vous pouvez également suspendre et relancer la synchronisation à tout moment. Si vous suspendez la synchronisation pendant plus de 28 jours, tous vos utilisateurs seront désactivés.

Configuration et gestion de votre étendue de synchronisation

Vous pouvez configurer votre étendue de synchronisation de l'une des manières suivantes :

- Configuration guidée : Si vous synchronisez vos utilisateurs et groupes depuis Active Directory vers IAM Identity Center pour la première fois, suivez les étapes décrites Configuration guidée pour configurer votre étendue de synchronisation. Une fois la configuration guidée terminée, vous pouvez modifier l'étendue de la synchronisation à tout moment en suivant les autres procédures décrites dans cette section.
- Si vous avez déjà des utilisateurs et des groupes synchronisés dans IAM Identity Center ou si vous ne souhaitez pas suivre la configuration guidée, choisissez Gérer la synchronisation. Ignorez la procédure de configuration guidée et suivez les autres procédures de cette section selon les besoins pour configurer et gérer votre étendue de synchronisation.

Procédures

- Configuration guidée
- Ajoutez des utilisateurs et des groupes à votre zone de synchronisation

- Supprimer des utilisateurs et des groupes de votre zone de synchronisation
- Pause et reprise de la synchronisation
- Configurez les mappages d'attributs pour votre synchronisation
- Automatisez votre configuration de synchronisation pour une synchronisation AD configurable

Configuration guidée

1. Ouvrez la console IAM Identity Center.

   > **Note**
   >
   > Assurez-vous que la console IAM Identity Center utilise l'un des emplacements Régions AWS où se trouve votre AWS Managed Microsoft AD répertoire avant de passer à l'étape suivante.

2. Sélectionnez Settings (Paramètres).
3. En haut de la page, dans le message de notification, choisissez Démarrer la configuration guidée.
4. À l'étape 1, facultatif : configurez les mappages d'attributs, passez en revue les mappages d'attributs par défaut pour les utilisateurs et les groupes. Si aucune modification n'est requise, choisissez Next. Si des modifications sont nécessaires, apportez-les, puis choisissez Enregistrer les modifications.
5. À l'étape 2, facultatif : configurer l'étendue de la synchronisation, cliquez sur l'onglet Utilisateurs. Entrez ensuite le nom d'utilisateur exact de l'utilisateur que vous souhaitez ajouter à votre étendue de synchronisation et choisissez Ajouter. Ensuite, choisissez l'onglet Groupes. Entrez le nom exact du groupe que vous souhaitez ajouter à votre étendue de synchronisation et choisissez Ajouter. Ensuite, choisissez Suivant. Si vous souhaitez ajouter des utilisateurs et des groupes à votre zone de synchronisation ultérieurement, n'apportez aucune modification et choisissez Next.
6. Dans Étape 3 : Vérifiez et enregistrez la configuration, confirmez vos mappages d'attributs dans Étape 1 : Mappages d'attributs et vos utilisateurs et groupes dans Étape 2 : Étendue de synchronisation. Choisissez Save configuration. Cela vous amène à la page Gérer la synchronisation.

Ajoutez des utilisateurs et des groupes à votre zone de synchronisation

Pour ajouter des utilisateurs

1. Ouvrez la console IAM Identity Center.
2. Sélectionnez Settings (Paramètres).
3. Sur la page Paramètres, choisissez l'onglet Source d'identité, sélectionnez Actions, puis sélectionnez Gérer la synchronisation.
4. Sur la page Gérer la synchronisation, choisissez l'onglet Utilisateurs, puis sélectionnez Ajouter des utilisateurs et des groupes.
5. Dans l'onglet Utilisateurs, sous Utilisateur, entrez le nom d'utilisateur exact et choisissez Ajouter.
6. Sous Utilisateurs et groupes ajoutés, passez en revue l'utilisateur que vous souhaitez ajouter.
7. Sélectionnez Envoyer.
8. Dans le panneau de navigation, choisissez utilisateurs.
9. Sur la page Utilisateurs, l'utilisateur que vous avez spécifié peut mettre un certain temps à apparaître dans la liste. Cliquez sur l'icône d'actualisation pour mettre à jour la liste des utilisateurs.

Pour ajouter des groupes

1. Ouvrez la console IAM Identity Center.
2. Sélectionnez Settings (Paramètres).
3. Sur la page Paramètres, choisissez l'onglet Source d'identité, sélectionnez Actions, puis sélectionnez Gérer la synchronisation.
4. Sur la page Gérer la synchronisation, choisissez l'onglet Groupes, puis sélectionnez Ajouter des utilisateurs et des groupes.
5. Cliquez sur l'onglet Groups (Groupes). Sous Groupe, entrez le nom exact du groupe et choisissez Ajouter.
6. Sous Utilisateurs et groupes ajoutés, passez en revue le groupe que vous souhaitez ajouter.
7. Sélectionnez Envoyer.
8. Dans le panneau de navigation, choisissez Groupes .
9. Sur la page Groupes, le groupe que vous avez spécifié peut prendre un certain temps pour apparaître dans la liste. Cliquez sur l'icône d'actualisation pour mettre à jour la liste des groupes.

Supprimer des utilisateurs et des groupes de votre zone de synchronisation

Pour plus d'informations sur ce qui se passe lorsque vous supprimez des utilisateurs et des groupes de votre zone de synchronisation, consultezComment fonctionne la synchronisation AD configurable.

Pour supprimer des utilisateurs

1. Ouvrez la console IAM Identity Center.
2. Sélectionnez Settings (Paramètres).
3. Sur la page Paramètres, choisissez l'onglet Source d'identité, sélectionnez Actions, puis sélectionnez Gérer la synchronisation.
4. Sélectionnez l'onglet Utilisateurs.
5. Sous Utilisateurs synchronisés, cochez la case à côté de l'utilisateur que vous souhaitez supprimer. Pour supprimer tous les utilisateurs, cochez la case à côté de Nom d'utilisateur.
6. Sélectionnez Remove (Supprimer).

Pour supprimer des groupes

1. Ouvrez la console IAM Identity Center.
2. Sélectionnez Settings (Paramètres).
3. Sur la page Paramètres, choisissez l'onglet Source d'identité, sélectionnez Actions, puis sélectionnez Gérer la synchronisation.
4. Cliquez sur l'onglet Groups (Groupes).
5. Sous Groupes dans l'étendue de synchronisation, cochez la case à côté de l'utilisateur que vous souhaitez supprimer. Pour supprimer tous les groupes, cochez la case à côté du nom du groupe.
6. Sélectionnez Remove (Supprimer).

Pause et reprise de la synchronisation

La suspension de votre synchronisation interrompt tous les futurs cycles de synchronisation et empêche que les modifications que vous apportez aux utilisateurs et aux groupes dans Active Directory ne soient reflétées dans IAM Identity Center. Une fois que vous avez repris la synchronisation, le cycle de synchronisation prend en compte ces modifications lors de la prochaine synchronisation planifiée.

Pour suspendre votre synchronisation

1. Ouvrez la console IAM Identity Center.
2. Sélectionnez Settings (Paramètres).
3. Sur la page Paramètres, choisissez l'onglet Source d'identité, sélectionnez Actions, puis sélectionnez Gérer la synchronisation.
4. Sous Gérer la synchronisation, choisissez Suspendre la synchronisation.

Pour reprendre votre synchronisation

1. Ouvrez la console IAM Identity Center.
2. Sélectionnez Settings (Paramètres).
3. Sur la page Paramètres, choisissez l'onglet Source d'identité, sélectionnez Actions, puis sélectionnez Gérer la synchronisation.
4. Sous Gérer la synchronisation, choisissez Reprendre la synchronisation.

> **Note**
>
> Si vous voyez Suspendre la synchronisation au lieu de Reprendre la synchronisation, la synchronisation entre Active Directory et IAM Identity Center a déjà repris.

Configurez les mappages d'attributs pour votre synchronisation

Pour plus d'informations sur les attributs disponibles, consultezMappages d'attributs pour le répertoire AWS Managed Microsoft AD.

Pour configurer les mappages d'attributs dans IAM Identity Center avec votre annuaire

1. Ouvrez la console IAM Identity Center.
2. Sélectionnez Settings (Paramètres).
3. Sur la page Paramètres, choisissez l'onglet Source d'identité, sélectionnez Actions, puis sélectionnez Gérer la synchronisation.
4. Sous Gérer la synchronisation, choisissez Afficher le mappage des attributs.
5. Sous Attributs utilisateur Active Directory, configurez les attributs du magasin d'identités IAM Identity Center et les attributs utilisateur Active Directory. Par exemple, vous souhaiterez peut-

être mapper l'attribut de banque d'identités IAM Identity Center `email` à l'attribut d'annuaire des utilisateurs Active Directory. `${objectguid}`

> **Note**
>
> Sous Attributs de groupe, les attributs du magasin d'identités IAM Identity Center et les attributs du groupe Active Directory ne peuvent pas être modifiés.

6. Sélectionnez Enregistrer les modifications. Cela vous ramène à la page Gérer la synchronisation.

Automatisez votre configuration de synchronisation pour une synchronisation AD configurable

Pour garantir que votre flux de travail automatisé fonctionne comme prévu avec la synchronisation AD configurable, nous vous recommandons de suivre les étapes suivantes pour automatiser la configuration de votre synchronisation.

Pour automatiser votre configuration de synchronisation pour une synchronisation AD configurable

1. Dans Active Directory, créez un groupe de synchronisation parent contenant tous les utilisateurs et groupes que vous souhaitez synchroniser dans IAM Identity Center. Par exemple, vous pouvez nommer le groupe IAM IdentityCenterAllUsersAndGroups.
2. Dans IAM Identity Center, ajoutez le groupe de synchronisation parent à votre liste de synchronisation configurable. IAM Identity Center synchronisera tous les utilisateurs, groupes, sous-groupes et membres de tous les groupes contenus dans le groupe de synchronisation parent.
3. Utilisez les actions de l'API de gestion des utilisateurs et des groupes Active Directory fournies par Microsoft pour ajouter ou supprimer des utilisateurs et des groupes du groupe de synchronisation parent.

Synchronisation AD avec IAM Identity Center

Avec IAM Identity Center AD sync, vous utilisez IAM Identity Center pour attribuer aux utilisateurs et aux groupes d'Active Directory l'accès aux Comptes AWS applications gérées ou aux applications AWS gérées par le client. Toutes les identités associées à des attributions sont automatiquement synchronisées dans IAM Identity Center.

Comment fonctionne IAM Identity Center AD Sync

IAM Identity Center actualise les données d'identité basées sur la publicité dans le magasin d'identités selon le processus suivant.

Création

Lorsque vous attribuez des utilisateurs, des groupes Comptes AWS ou des applications à l'aide de la AWS console ou des appels d'API d'attribution, les informations relatives aux utilisateurs, aux groupes et aux membres sont périodiquement synchronisées dans la banque d'identités d'IAM Identity Center. Les utilisateurs ou les groupes ajoutés aux attributions du IAM Identity Center apparaissent généralement dans le magasin AWS d'identités dans les deux heures. En fonction de la quantité de données synchronisées, ce processus peut prendre plus de temps. Seuls les utilisateurs et les groupes auxquels un accès est directement attribué, ou qui sont membres d'un groupe auquel un accès est attribué, sont synchronisés.

Les groupes membres d'autres groupes (appelés groupes imbriqués) sont également enregistrés dans le magasin d'identités. Lorsque vous attribuez des attributions à un groupe dans Active Directory qui contient des groupes imbriqués, la manière dont les attributions sont appliquées varie selon que vous utilisez AD Sync ou AD Sync configurable.

- Synchronisation AD : lorsque vous attribuez des attributions à un groupe dans Active Directory qui contient des groupes imbriqués, seuls les membres directs du groupe peuvent accéder au compte. Par exemple, si vous accordez l'accès au groupe A et que le groupe B est membre du groupe A, seuls les membres directs du groupe A peuvent accéder au compte. Aucun membre du groupe B n'hérite de cet accès.
- Synchronisation AD configurable : l'utilisation de la synchronisation AD configurable pour attribuer des attributions à un groupe dans Active Directory contenant des groupes imbriqués peut augmenter le nombre d'utilisateurs ayant accès aux applications Comptes AWS ou à celles-ci. Dans ce cas, l'attribution s'applique à tous les utilisateurs, y compris ceux des groupes imbriqués. Par exemple, si vous accordez l'accès au groupe A et que le groupe B est membre du groupe A, les membres du groupe B héritent également de cet accès.

Si un utilisateur accède à IAM Identity Center avant que son objet utilisateur n'ait été synchronisé pour la première fois, l'objet de la banque d'identités de cet utilisateur est créé à la demande à l'aide du provisionnement just-in-time (JIT). Les utilisateurs créés par le provisionnement JIT ne sont pas synchronisés sauf s'ils disposent de droits IAM Identity Center directement attribués ou basés sur

des groupes. Les adhésions à des groupes pour les utilisateurs approvisionnés par JIT ne sont pas disponibles avant la synchronisation.

Pour obtenir des instructions sur la façon d'attribuer l'accès aux utilisateurs Comptes AWS, consultezAccès par authentification unique à Comptes AWS.

Mettre à jour

Les données d'identité de la banque d'identités d'IAM Identity Center restent actualisées en lisant régulièrement les données du répertoire source dans Active Directory. Les données d'identité modifiées dans Active Directory apparaissent généralement dans le magasin AWS d'identités dans les quatre heures. En fonction de la quantité de données synchronisées, ce processus peut prendre plus de temps.

Les objets d'utilisateur et de groupe et leurs appartenances sont créés ou mis à jour dans IAM Identity Center pour être mappés aux objets correspondants dans le répertoire source d'Active Directory. Pour les attributs utilisateur, seul le sous-ensemble d'attributs répertorié dans la section Gérer les attributs pour le contrôle d'accès de la console IAM Identity Center est mis à jour dans IAM Identity Center. En outre, les attributs utilisateur sont mis à jour à chaque événement d'authentification utilisateur.

Suppression

Les utilisateurs et les groupes sont supprimés de la banque d'identités IAM Identity Center lorsque les objets d'utilisateur ou de groupe correspondants sont supprimés du répertoire source dans Active Directory.

Connectez-vous à un fournisseur d'identité externe

Si vous utilisez un annuaire autogéré dans Active Directory ou un AWS Managed Microsoft AD, consultezSe connecter à un Microsoft AD annuaire. Pour les autres fournisseurs d'identité externes (IdPs), vous pouvez les utiliser AWS IAM Identity Center pour authentifier les identités IdPs via la norme SAML (Security Assertion Markup Language) 2.0. Cela permet à vos utilisateurs de se connecter au portail AWS d'accès avec leurs informations d'identification professionnelles. Ils peuvent ensuite accéder aux comptes, rôles et applications qui leur sont assignés et hébergés en externe IdPs.

Par exemple, vous pouvez connecter un IdP externe tel que Okta ou à IAM Microsoft Entra ID Identity Center. Vos utilisateurs peuvent ensuite se connecter au portail d' AWS accès avec leurs

informations d'identification existantes Okta ou leurs Microsoft Entra ID informations d'identification. Pour contrôler ce que vos utilisateurs peuvent faire une fois qu'ils sont connectés, vous pouvez leur attribuer des autorisations d'accès de manière centralisée pour tous les comptes et applications de votre AWS organisation. En outre, les développeurs peuvent simplement se connecter au AWS Command Line Interface (AWS CLI) à l'aide de leurs informations d'identification existantes et bénéficier de la génération et de la rotation automatiques des informations d'identification à court terme.

Le protocole SAML ne permet pas d'interroger l'IdP pour en savoir plus sur les utilisateurs et les groupes. Par conséquent, vous devez informer IAM Identity Center de l'existence de ces utilisateurs et groupes en les configurant dans IAM Identity Center.

Provisionnement lorsque les utilisateurs proviennent d'un IdP externe

Lorsque vous utilisez un IdP externe, vous devez configurer tous les utilisateurs et groupes concernés dans IAM Identity Center avant de pouvoir attribuer des tâches à des applications ou à Comptes AWS des applications. Pour ce faire, vous pouvez configurer Approvisionnement automatique pour vos utilisateurs et groupes, ou utiliserApprovisionnement manuel. Quelle que soit la manière dont vous configurez les utilisateurs, IAM Identity Center redirige l' AWS Management Console interface de ligne de commande et l'authentification des applications vers votre IdP externe. IAM Identity Center accorde ensuite l'accès à ces ressources en fonction des politiques que vous créez dans IAM Identity Center. Pour plus d'informations sur le provisionnement, consultezProvisionnement d'utilisateurs et de groupes.

Comment se connecter à un fournisseur d'identité externe

Des step-by-step didacticiels sont disponibles pour les personnes prises en charge IdPs :

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

Il existe différents prérequis, considérations et procédures de provisionnement pour les différents systèmes externes pris en charge. IdPs La procédure suivante fournit un aperçu général de la procédure utilisée avec tous les fournisseurs d'identité externes.

Pour vous connecter à un fournisseur d'identité externe

1. Ouvrez la console IAM Identity Center.
2. Sélectionnez Settings (Paramètres).
3. Sur la page Paramètres, choisissez l'onglet Source d'identité, puis sélectionnez Actions > Modifier la source d'identité.
4. Sous Choisir une source d'identité, sélectionnez Fournisseur d'identité externe, puis cliquez sur Suivant.
5. Sous Configurer le fournisseur d'identité externe, procédez comme suit :

    a. Sous Métadonnées du fournisseur de services, choisissez Télécharger le fichier de métadonnées pour télécharger le fichier de métadonnées et l'enregistrer sur votre système. Le fichier de métadonnées SAML d'IAM Identity Center est requis par votre fournisseur d'identité externe.

    b. Sous Métadonnées du fournisseur d'identité, choisissez Choisir un fichier et recherchez le fichier de métadonnées que vous avez téléchargé auprès de votre fournisseur d'identité externe. Téléchargez ensuite le fichier. Ce fichier de métadonnées contient le certificat public x509 nécessaire utilisé pour approuver les messages envoyés par l'IdP.

    c. Choisissez Suivant.

    > **Important**
    >
    > La modification de votre source vers ou depuis Active Directory supprime toutes les attributions d'utilisateurs et de groupes existantes. Vous devez réappliquer les assignations manuellement une fois que vous avez correctement modifié votre source.

6. Après avoir lu la clause de non-responsabilité et être prêt à continuer, saisissez ACCEPTER.
7. Choisissez Modifier la source d'identité. Un message d'état vous informe que vous avez correctement modifié la source d'identité.

Rubriques

- Utilisation de la fédération d'identité SAML et SCIM avec des fournisseurs d'identité externes
- Profil SCIM et implémentation de SAML 2.0

Utilisation de la fédération d'identité SAML et SCIM avec des fournisseurs d'identité externes

IAM Identity Center met en œuvre les protocoles normalisés suivants pour la fédération des identités :

- SAML 2.0 pour l'authentification des utilisateurs
- SCIM pour le provisionnement

Tout fournisseur d'identité (IdP) qui implémente ces protocoles standard est censé interagir avec succès avec IAM Identity Center, en tenant compte des considérations particulières suivantes :

- SAML
  - IAM Identity Center nécessite un format SAML NameID pour l'adresse e-mail (c'est-à-dire,). `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`
  - La valeur du champ NameID dans les assertions doit être une chaîne conforme à la norme RFC 2822 (https://tools.ietf.org/html/rfc2822) addr-spec (« ») (https://tools.ietf.org/html/rfc2822#section-3.4.1). `name@domain.com`
  - Le fichier de métadonnées ne doit pas comporter plus de 75 000 caractères.
  - Les métadonnées doivent contenir un EntityID, un certificat X509 et faire partie de SingleSignOnService l'URL de connexion.
  - Aucune clé de chiffrement n'est prise en charge.

- SCIM
  - La mise en œuvre du SCIM d'IAM Identity Center est basée sur les RFC SCIM 7642 (https://tools.ietf.org/html/rfc7642), 7643 (https://tools.ietf.org/html/rfc7643) et 7644 (https://tools.ietf.org/html/rfc7644), ainsi que sur les exigences d'interopérabilité énoncées dans le projet de mars 2020 du profil SCIM de FastFed base 1.0 (https://openid.net/specs/fastfed-scim-1_0-02.html#rfc.section.4). Toute différence entre ces documents et l'implémentation actuelle dans IAM Identity Center est décrite dans la section Opérations d'API prises en charge du guide du développeur de mise en œuvre d'IAM Identity Center SCIM.

IdPs qui ne sont pas conformes aux normes et aux considérations mentionnées ci-dessus ne sont pas prises en charge. Veuillez contacter votre IdP pour toute question ou précision concernant la conformité de ses produits à ces normes et considérations.

Si vous rencontrez des problèmes pour connecter votre IdP à IAM Identity Center, nous vous recommandons de vérifier :

- AWS CloudTrail enregistre en filtrant sur le nom de l'événement ExternalIdP DirectoryLogin
- Journaux spécifiques à l'IDP et/ou journaux de débogage
- Résolution des problèmes liés à IAM Identity Center

> **Note**
>
> Certains IdPs, comme ceux présentés dans leTutoriels de mise en route, offrent une expérience de configuration simplifiée pour IAM Identity Center sous la forme d'une « application » ou d'un « connecteur » spécialement conçu pour IAM Identity Center. Si votre IdP propose cette option, nous vous recommandons de l'utiliser, en prenant soin de choisir l'élément spécialement conçu pour IAM Identity Center. D'autres éléments appelés « AWS », « AWS fédération » ou noms génériques similaires « »AWS peuvent utiliser d'autres approches de fédération et/ou points de terminaison et peuvent ne pas fonctionner comme prévu avec IAM Identity Center.

Profil SCIM et implémentation de SAML 2.0

SCIM et SAML sont des éléments importants à prendre en compte lors de la configuration d'IAM Identity Center.

Implémentation de SAML 2.0

IAM Identity Center prend en charge la fédération des identités avec le langage SAML (Security Assertion Markup Language) 2.0. Cela permet à IAM Identity Center d'authentifier les identités auprès de fournisseurs d'identité externes ()IdPs. SAML 2.0 est un standard ouvert utilisé pour échanger des assertions SAML en toute sécurité. SAML 2.0 transmet des informations sur un utilisateur entre une autorité SAML (appelée fournisseur d'identité ou IdP) et un consommateur SAML (appelé fournisseur de services ou SP). Le service IAM Identity Center utilise ces informations pour fournir une authentification unique fédérée. L'authentification unique permet aux utilisateurs d'accéder

aux applications Comptes AWS et de les configurer en fonction de leurs informations d'identification de fournisseur d'identité existantes.

IAM Identity Center ajoute des fonctionnalités IDP SAML à votre boutique IAM Identity Center ou à un fournisseur AWS Managed Microsoft AD d'identité externe. Les utilisateurs peuvent ensuite se connecter de manière unique aux services qui prennent en charge le protocole SAML, y compris les applications tierces telles que Microsoft 365Concur, AWS Management Console et. Salesforce

Le protocole SAML ne permet toutefois pas d'interroger l'IdP pour en savoir plus sur les utilisateurs et les groupes. Par conséquent, vous devez informer IAM Identity Center de l'existence de ces utilisateurs et groupes en les configurant dans IAM Identity Center.

profil SCIM

IAM Identity Center prend en charge la norme SCIM (System for Cross-Domain Identity Management) v2.0. Le SCIM synchronise les identités de votre IAM Identity Center avec celles de votre IdP. Cela inclut le provisionnement, les mises à jour et le déprovisionnement des utilisateurs entre votre IdP et IAM Identity Center.

Pour plus d'informations sur la mise en œuvre du SCIM, consultezApprovisionnement automatique. Pour plus de détails sur la mise en œuvre du SCIM par IAM Identity Center, consultez le guide du développeur de mise en œuvre du SCIM d'IAM Identity Center.

Rubriques

- Approvisionnement automatique
- Approvisionnement manuel
- Gestion des certificats SAML 2.0

Approvisionnement automatique

IAM Identity Center prend en charge le provisionnement automatique (synchronisation) des informations sur les utilisateurs et les groupes depuis votre fournisseur d'identité (IdP) vers IAM Identity Center à l'aide du protocole System for Cross-domain Identity Management (SCIM) v2.0. Lorsque vous configurez la synchronisation SCIM, vous créez un mappage des attributs utilisateur de votre fournisseur d'identité (IdP) avec les attributs nommés dans IAM Identity Center. Cela entraîne la correspondance des attributs attendus entre IAM Identity Center et votre IdP. Vous configurez cette connexion dans votre IdP à l'aide de votre point de terminaison SCIM pour IAM Identity Center et d'un jeton porteur que vous créez dans IAM Identity Center.

Rubriques

Considérations relatives à l'utilisation du provisionnement automatique

Avant de commencer à déployer le SCIM, nous vous recommandons de prendre d'abord en compte les considérations importantes suivantes concernant son fonctionnement avec IAM Identity Center. Pour d'autres considérations relatives au provisionnement, consultez la section Tutoriels de mise en route applicable à votre IdP.

- Si vous fournissez une adresse e-mail principale, cette valeur d'attribut doit être unique pour chaque utilisateur. Dans certains IdPs cas, l'adresse e-mail principale peut ne pas être une adresse e-mail réelle. Par exemple, il peut s'agir d'un nom principal universel (UPN) qui ressemble uniquement à un e-mail. Ils IdPs peuvent avoir une adresse e-mail secondaire ou « autre » contenant la véritable adresse e-mail de l'utilisateur. Vous devez configurer le SCIM dans votre IdP pour associer l'adresse e-mail unique non NULL à l'attribut d'adresse e-mail principale du IAM Identity Center. Et vous devez associer l'identifiant de connexion unique non NULL de l'utilisateur à l'attribut de nom d'utilisateur IAM Identity Center. Vérifiez si votre IdP possède une valeur unique qui est à la fois l'identifiant de connexion et le nom e-mail de l'utilisateur. Si tel est le cas, vous pouvez mapper ce champ IdP à la fois à l'adresse e-mail principale et au nom d'utilisateur de l'IAM Identity Center.
- Pour que la synchronisation SCIM fonctionne, chaque utilisateur doit avoir un prénom, un nom de famille, un nom d'utilisateur et une valeur de nom d'affichage spécifiés. Si l'une de ces valeurs est absente pour un utilisateur, celui-ci ne sera pas approvisionné.
- Si vous devez utiliser des applications tierces, vous devez d'abord mapper l'attribut de sujet SAML sortant à l'attribut de nom d'utilisateur. Si l'application tierce a besoin d'une adresse e-mail routable, vous devez fournir l'attribut e-mail à votre IdP.
- Les intervalles de mise en service et de mise à jour du SCIM sont contrôlés par votre fournisseur d'identité. Les modifications apportées aux utilisateurs et aux groupes de votre fournisseur

d'identité ne sont reflétées dans IAM Identity Center qu'une fois que votre fournisseur d'identité a envoyé ces modifications à IAM Identity Center. Consultez votre fournisseur d'identité pour plus de détails sur la fréquence des mises à jour des utilisateurs et des groupes.

- Actuellement, les attributs à valeurs multiples (tels que plusieurs e-mails ou numéros de téléphone pour un utilisateur donné) ne sont pas fournis avec SCIM. Les tentatives de synchronisation d'attributs à valeurs multiples dans IAM Identity Center avec SCIM échoueront. Pour éviter les échecs, assurez-vous qu'une seule valeur est transmise pour chaque attribut. Si vous avez des utilisateurs dotés d'attributs à valeurs multiples, supprimez ou modifiez les mappages d'attributs dupliqués dans SCIM sur votre IdP pour la connexion à IAM Identity Center.
- Vérifiez que le mappage `externalId` SCIM de votre IdP correspond à une valeur unique, toujours présente et peu susceptible de changer pour vos utilisateurs. Par exemple, votre IdP peut fournir un identifiant garanti `objectId` ou autre qui n'est pas affecté par les modifications apportées aux attributs utilisateur tels que le nom et l'adresse e-mail. Si tel est le cas, vous pouvez mapper cette valeur au `externalId` champ SCIM. Cela garantit que vos utilisateurs ne perdront pas leurs AWS droits, attributions ou autorisations si vous devez modifier leur nom ou leur adresse e-mail.
- Utilisateurs qui n'ont pas encore été affectés à une application ou qui Compte AWS ne peuvent pas être approvisionnés dans IAM Identity Center. Pour synchroniser les utilisateurs et les groupes, assurez-vous qu'ils sont affectés à l'application ou à une autre configuration représentant la connexion de votre IdP à IAM Identity Center.
- Le comportement de déprovisionnement des utilisateurs est géré par le fournisseur d'identité et peut varier en fonction de sa mise en œuvre. Renseignez-vous auprès de votre fournisseur d'identité pour en savoir plus sur le déprovisionnement des utilisateurs.

Pour plus d'informations sur la mise en œuvre du SCIM par IAM Identity Center, consultez le guide du développeur de mise en œuvre du SCIM d'IAM Identity Center.

Comment surveiller l'expiration des jetons d'accès

Les jetons d'accès SCIM sont générés avec une validité d'un an. Lorsque votre jeton d'accès SCIM doit expirer dans 90 jours ou moins, il vous AWS envoie des rappels dans la console IAM Identity Center et via le tableau de AWS Health bord pour vous aider à faire pivoter le jeton. En faisant pivoter le jeton d'accès SCIM avant son expiration, vous sécurisez en permanence le provisionnement automatique des informations sur les utilisateurs et les groupes. Si le jeton d'accès SCIM expire, la synchronisation des informations relatives aux utilisateurs et aux groupes entre votre fournisseur d'identité et IAM Identity Center s'arrête, de sorte que le provisionnement automatique ne peut plus effectuer de mises à jour ni créer et supprimer des informations. L'interruption du provisionnement

automatique peut entraîner des risques de sécurité accrus et avoir un impact sur l'accès à vos services.

Les rappels de la console Identity Center sont conservés jusqu'à ce que vous fassiez pivoter le jeton d'accès SCIM et que vous supprimiez tous les jetons d'accès inutilisés ou expirés. Les événements du tableau de AWS Health bord sont renouvelés chaque semaine entre 90 et 60 jours, deux fois par semaine de 60 à 30 jours, trois fois par semaine de 30 à 15 jours et tous les jours pendant 15 jours jusqu'à l'expiration des jetons d'accès SCIM.

Comment activer le provisionnement automatique

Utilisez la procédure suivante pour activer le provisionnement automatique des utilisateurs et des groupes depuis votre IdP vers IAM Identity Center à l'aide du protocole SCIM.

> **Note**
>
> Avant de commencer cette procédure, nous vous recommandons de passer d'abord en revue les considérations de provisionnement applicables à votre IdP. Pour plus d'informations, consultez le correspondant Tutoriels de mise en route à votre IdP.

Pour activer le provisionnement automatique dans IAM Identity Center

1. Une fois que vous avez rempli les conditions requises, ouvrez la console IAM Identity Center.
2. Choisissez Paramètres dans le volet de navigation de gauche.
3. Sur la page Paramètres, recherchez la zone Informations de provisionnement automatique, puis choisissez Activer. Cela active immédiatement le provisionnement automatique dans IAM Identity Center et affiche les informations nécessaires sur le point de terminaison SCIM et le jeton d'accès.
4. Dans la boîte de dialogue de provisionnement automatique entrant, copiez chacune des valeurs des options suivantes. Vous devrez les coller ultérieurement lorsque vous configurerez le provisionnement dans votre IdP.
   a. Point de terminaison SCIM
   b. Jeton d'accès
5. Choisissez Fermer.

Une fois cette procédure terminée, vous devez configurer le provisionnement automatique dans votre IdP. Pour plus d'informations, consultez le correspondant Tutoriels de mise en route à votre IdP.

Comment désactiver le provisionnement automatique

Utilisez la procédure suivante pour désactiver le provisionnement automatique dans la console IAM Identity Center.

> **Important**
>
> Vous devez supprimer le jeton d'accès avant de commencer cette procédure. Pour plus d'informations, consultez Comment supprimer un jeton d'accès.

Pour désactiver le provisionnement automatique dans la console IAM Identity Center

1. Dans la console IAM Identity Center, sélectionnez Paramètres dans le volet de navigation de gauche.
2. Sur la page Paramètres, choisissez l'onglet Source d'identité, puis sélectionnez Actions > Gérer le provisionnement.
3. Sur la page Provisionnement automatique, choisissez Désactiver.
4. Dans la boîte de dialogue Désactiver le provisionnement automatique, passez en revue les informations, tapez DISABLE, puis choisissez Désactiver le provisionnement automatique.

Comment générer un nouveau jeton d'accès

Utilisez la procédure suivante pour générer un nouveau jeton d'accès dans la console IAM Identity Center.

> **Note**
>
> Cette procédure nécessite que vous ayez préalablement activé le provisionnement automatique. Pour plus d'informations, consultez Comment activer le provisionnement automatique.

Pour générer un nouveau jeton d'accès

1. Dans la console IAM Identity Center, sélectionnez Paramètres dans le volet de navigation de gauche.
2. Sur la page Paramètres, choisissez l'onglet Source d'identité, puis sélectionnez Actions > Gérer le provisionnement.
3. Sur la page Provisionnement automatique, sous Jetons d'accès, choisissez Générer un jeton.
4. Dans la boîte de dialogue Générer un nouveau jeton d'accès, copiez le nouveau jeton d'accès et enregistrez-le en lieu sûr.
5. Choisissez Fermer.

Comment supprimer un jeton d'accès

Utilisez la procédure suivante pour supprimer un jeton d'accès existant dans la console IAM Identity Center.

Pour supprimer un jeton d'accès existant

1. Dans la console IAM Identity Center, sélectionnez Paramètres dans le volet de navigation de gauche.
2. Sur la page Paramètres, choisissez l'onglet Source d'identité, puis sélectionnez Actions > Gérer le provisionnement.
3. Sur la page Provisionnement automatique, sous Jetons d'accès, sélectionnez le jeton d'accès que vous souhaitez supprimer, puis choisissez Supprimer.
4. Dans la boîte de dialogue Supprimer le jeton d'accès, passez en revue les informations, tapez DELETE, puis choisissez Supprimer le jeton d'accès.

Comment faire pivoter un jeton d'accès

Un annuaire IAM Identity Center prend en charge jusqu'à deux jetons d'accès à la fois. Pour générer un jeton d'accès supplémentaire avant toute rotation, supprimez tous les jetons d'accès expirés ou non utilisés.

Si votre jeton d'accès SCIM est sur le point d'expirer, vous pouvez utiliser la procédure suivante pour faire pivoter un jeton d'accès existant dans la console IAM Identity Center.

Pour faire pivoter un jeton d'accès

1. Dans la console IAM Identity Center, sélectionnez Paramètres dans le volet de navigation de gauche.
2. Sur la page Paramètres, choisissez l'onglet Source d'identité, puis sélectionnez Actions > Gérer le provisionnement.
3. Sur la page Provisionnement automatique, sous Jetons d'accès, notez l'ID du jeton que vous souhaitez faire pivoter.
4. Suivez les étapes décrites Comment générer un nouveau jeton d'accès pour créer un nouveau jeton. Si vous avez déjà créé le nombre maximum de jetons d'accès SCIM, vous devez d'abord supprimer l'un des jetons existants.
5. Accédez au site Web de votre fournisseur d'identité et configurez le nouveau jeton d'accès pour le provisionnement SCIM, puis testez la connectivité à IAM Identity Center à l'aide du nouveau jeton d'accès SCIM. Une fois que vous avez confirmé que le provisionnement fonctionne correctement à l'aide du nouveau jeton, passez à l'étape suivante de cette procédure.
6. Suivez les étapes décrites Comment supprimer un jeton d'accès pour supprimer l'ancien jeton d'accès que vous avez indiqué précédemment. Vous pouvez également utiliser la date de création du jeton comme indication du jeton à supprimer.

Approvisionnement manuel

Certains IdPs ne sont pas compatibles avec le système de gestion des identités interdomaines (SCIM) ou ont une implémentation SCIM incompatible. Dans ces cas, vous pouvez configurer manuellement les utilisateurs via la console IAM Identity Center. Lorsque vous ajoutez des utilisateurs à IAM Identity Center, assurez-vous de définir le nom d'utilisateur de manière à ce qu'il soit identique au nom d'utilisateur que vous avez dans votre IdP. Au minimum, vous devez disposer d'une adresse e-mail et d'un nom d'utilisateur uniques. Pour plus d'informations, consultez Unicité du nom d'utilisateur et de l'adresse e-mail.

Vous devez également gérer tous les groupes manuellement dans IAM Identity Center. Pour ce faire, vous devez créer les groupes et les ajouter à l'aide de la console IAM Identity Center. Ces groupes n'ont pas besoin de correspondre à ce qui existe dans votre IdP. Pour plus d'informations, consultez Groups.

Gestion des certificats SAML 2.0

IAM Identity Center utilise des certificats pour établir une relation de confiance SAML entre IAM Identity Center et votre fournisseur d'identité externe (IdP). Lorsque vous ajoutez un IdP externe dans IAM Identity Center, vous devez également obtenir au moins un certificat public SAML 2.0 X.509 auprès de l'IdP externe. Ce certificat est généralement installé automatiquement lors de l'échange de métadonnées IDP SAML lors de la création de la confiance.

En tant qu'administrateur du centre d'identité IAM, vous devrez parfois remplacer les anciens certificats IdP par des certificats plus récents. Par exemple, il se peut que vous deviez remplacer un certificat IdP lorsque la date d'expiration du certificat approche. Le processus de remplacement d'un ancien certificat par un nouveau est appelé rotation des certificats.

Rubriques

Faire pivoter un certificat SAML 2.0

Il se peut que vous deviez importer des certificats périodiquement afin de remplacer les certificats non valides ou expirés émis par votre fournisseur d'identité. Cela permet d'éviter toute interruption ou interruption de l'authentification. Tous les certificats importés sont automatiquement actifs. Les certificats ne doivent être supprimés qu'après avoir vérifié qu'ils ne sont plus utilisés par le fournisseur d'identité associé.

Vous devez également tenir compte du fait que certains IdPs peuvent ne pas prendre en charge plusieurs certificats. Dans ce cas, le fait d'alterner les certificats avec ces derniers IdPs peut entraîner une interruption de service temporaire pour vos utilisateurs. Le service est rétabli lorsque la confiance avec cet IdP a été rétablie avec succès. Planifiez cette opération avec soin en dehors des heures de pointe si possible.

> **Note**
>
> Pour des raisons de sécurité, dès que des signes de compromission ou de mauvaise gestion d'un certificat SAML existant apparaissent, vous devez immédiatement le supprimer et le faire pivoter.

La rotation d'un certificat IAM Identity Center est un processus en plusieurs étapes qui implique les étapes suivantes :

- Obtenir un nouveau certificat auprès de l'IdP
- Importation du nouveau certificat dans IAM Identity Center
- Activation du nouveau certificat dans l'IdP
- Supprimer l'ancien certificat

Utilisez toutes les procédures suivantes pour terminer le processus de rotation des certificats tout en évitant toute interruption de l'authentification.

Étape 1 : obtenir un nouveau certificat auprès de l'IdP

Accédez au site Web de l'IdP et téléchargez leur certificat SAML 2.0. Assurez-vous que le fichier de certificat est téléchargé au format PEM codé. La plupart des fournisseurs vous permettent de créer plusieurs certificats SAML 2.0 dans l'IdP. Il est probable qu'ils soient marqués comme désactivés ou inactifs.

Étape 2 : Importer le nouveau certificat dans IAM Identity Center

Utilisez la procédure suivante pour importer le nouveau certificat à l'aide de la console IAM Identity Center.

1. Dans la console IAM Identity Center, sélectionnez Paramètres.
2. Sur la page Paramètres, choisissez l'onglet Source d'identité, puis sélectionnez Actions > Gérer l'authentification.
3. Sur la page Gérer les certificats SAML 2.0, choisissez Importer le certificat.
4. Dans la boîte de dialogue Importer un certificat SAML 2.0, choisissez Choisir un fichier, accédez à votre fichier de certificat et sélectionnez-le, puis choisissez Importer un certificat.

À ce stade, IAM Identity Center fera confiance à tous les messages SAML entrants signés à partir des deux certificats que vous avez importés.

Étape 3 : activer le nouveau certificat dans l'IdP

Retournez sur le site Web de l'IdP et marquez le nouveau certificat que vous avez créé précédemment comme principal ou actif. À ce stade, tous les messages SAML signés par l'IdP doivent utiliser le nouveau certificat.

Étape 4 : Supprimer l'ancien certificat

Suivez la procédure ci-dessous pour terminer le processus de rotation des certificats pour votre IdP. Il doit toujours y avoir au moins un certificat valide répertorié, et il ne peut pas être supprimé.

> **Note**
>
> Assurez-vous que votre fournisseur d'identité ne signe plus les réponses SAML avec ce certificat avant de le supprimer.

1. Sur la page Gérer les certificats SAML 2.0, sélectionnez le certificat que vous souhaitez supprimer. Sélectionnez Delete (Supprimer).
2. Dans la boîte de dialogue Supprimer le certificat SAML 2.0, tapez **DELETE** pour confirmer, puis choisissez Supprimer.
3. Retournez sur le site Web de l'IdP et effectuez les étapes nécessaires pour supprimer l'ancien certificat inactif.

Indicateurs du statut d'expiration des certificats

Sur la page Gérer les certificats SAML 2.0, vous remarquerez peut-être des icônes d'indicateur d'état colorées. Ces icônes apparaissent dans la colonne Expire le jour à côté de chaque certificat de la liste. Ce qui suit décrit les critères utilisés par IAM Identity Center pour déterminer quelle icône est affichée pour chaque certificat.

- Rouge — Indique qu'un certificat est actuellement expiré.
- Jaune — Indique qu'un certificat expirera dans 90 jours ou moins.
- Vert — Indique qu'un certificat est actuellement valide et le restera pendant au moins 90 jours supplémentaires.

Pour vérifier l'état actuel d'un certificat

1. Dans la console IAM Identity Center, sélectionnez Paramètres.
2. Sur la page Paramètres, choisissez l'onglet Source d'identité, puis sélectionnez Actions > Gérer l'authentification.
3. Sur la page Gérer l'authentification SAML 2.0, sous Gérer les certificats SAML 2.0, vérifiez le statut des certificats dans la liste, comme indiqué dans la colonne Expire le.

Utilisation du portail AWS d'accès

Le portail AWS d'accès vous fournit (utilisateurs finaux) un accès par authentification unique à toutes vos applications cloud Comptes AWS et aux applications cloud les plus couramment utilisées, telles qu'Office 365, Concur, Salesforce et bien d'autres encore. Vous pouvez lancer rapidement plusieurs applications en cliquant simplement sur l'icône Compte AWS ou de l'application dans le portail. La présence d'icônes d'applications dans votre portail AWS d'accès signifie qu'un administrateur de votre entreprise vous a accordé l'accès à ces applications Comptes AWS ou à ces applications. Cela signifie également que vous pouvez accéder à tous ces comptes ou applications depuis le portail AWS d'accès sans demander de connexion supplémentaire.

Contactez votre administrateur pour demander un accès supplémentaire dans les situations suivantes :

- Aucune application Compte AWS ou application à laquelle vous devez accéder ne s'affiche.
- L'accès que vous avez à un compte ou à une application donné n'est pas celui que vous attendiez.

Rubriques

Acceptation de l'invitation à rejoindre IAM Identity Center

Si c'est la première fois que vous vous connectez au portail AWS d'accès, consultez vos e-mails pour obtenir des instructions sur la façon d'activer vos informations d'identification d'utilisateur.

Pour activer vos informations d'identification d'utilisateur

1. En fonction de l'e-mail que vous avez reçu de votre entreprise, choisissez l'une des méthodes suivantes pour activer vos informations d'identification utilisateur afin de pouvoir commencer à utiliser le portail AWS d'accès.

   a. Si vous avez reçu un e-mail avec pour objet Invitation à rejoindre AWS IAM Identity Center (successeur de Single Sign-On), ouvrez-le et choisissez Accepter l'invitation. AWS Sur la page d'inscription d'un nouvel utilisateur, entrez et confirmez un mot de passe, puis choisissez Définir un nouveau mot de passe. Vous utiliserez ce mot de passe chaque fois que vous vous connecterez au portail.

   b. Si le support informatique ou l'administrateur informatique de votre entreprise vous ont envoyé un e-mail, suivez les instructions fournies pour activer vos informations d'identification utilisateur.

2. Une fois que vous avez activé vos informations d'identification d'utilisateur en fournissant un nouveau mot de passe, le portail d' AWS accès vous connecte automatiquement. Si ce n'est pas le cas, vous pouvez vous connecter manuellement au portail AWS d'accès en suivant les instructions fournies dans la section suivante.

Connexion au portail d' AWS accès

À ce stade, un administrateur devrait vous avoir fourni une URL de connexion spécifique AWS au portail d'accès. Une fois que vous avez obtenu cette URL, vous pouvez vous connecter au portail. Pour plus d'informations, voir Se connecter au portail AWS d'accès.

> **Note**
>
> Une fois connecté, la durée par défaut de votre session AWS au portail d'accès est de 8 heures. Sachez qu'un administrateur peut modifier la durée de cette session.

Appareils approuvés

Lorsque vous choisissez l'option Ceci est un appareil fiable sur la page de connexion, IAM Identity Center considère toutes les futures connexions à partir de cet appareil comme autorisées. Cela signifie qu'IAM Identity Center ne proposera pas d'option permettant de saisir un code MFA tant que

vous utilisez cet appareil fiable. Il existe toutefois certaines exceptions, notamment la connexion à partir d'un nouveau navigateur ou l'attribution d'une adresse IP inconnue à votre appareil.

Conseils de connexion pour le portail AWS d'accès

Voici quelques conseils pour vous aider à gérer l'expérience de votre portail d' AWS accès.

- Il peut arriver que vous deviez vous déconnecter puis vous reconnecter au portail AWS d'accès. Cela peut être nécessaire pour accéder aux nouvelles applications que votre administrateur vous a récemment attribuées. Ce n'est toutefois pas obligatoire, car toutes les nouvelles applications sont actualisées toutes les heures.
- Lorsque vous vous connectez au portail AWS d'accès, vous pouvez ouvrir n'importe laquelle des applications répertoriées dans le portail en choisissant l'icône de l'application. Une fois que vous avez terminé d'utiliser l'application, vous pouvez fermer l'application ou vous déconnecter du portail AWS d'accès. Si vous vous contentez de fermer l'application, vous n'êtes pas déconnecté du portail utilisateur. Toutes les autres applications que vous avez ouvertes depuis le portail AWS d'accès restent ouvertes et en cours d'exécution.
- Avant de pouvoir vous connecter en tant qu'utilisateur différent, vous devez d'abord vous déconnecter du portail AWS d'accès. Lorsque vous vous déconnectez du portail utilisateur, toutes vos informations d'identification sont supprimées de la session du navigateur.
- Une fois connecté au portail AWS d'accès, vous pouvez passer à un rôle. Le changement de rôle met temporairement de côté vos autorisations d'utilisateur d'origine et vous donne à la place les autorisations attribuées au rôle. Pour plus d'informations, consultez Changement de rôles (console).

Déconnexion du portail AWS d'accès

Lorsque vous vous déconnectez du portail utilisateur, vos informations d'identification sont entièrement supprimées de la session du navigateur. Pour plus d'informations, voir Déconnexion du portail AWS d'accès dans le Connexion à AWSguide.

Pour vous déconnecter du portail AWS d'accès

- Dans le portail AWS d'accès, choisissez Se déconnecter dans la barre de navigation.

> **Note**
>
> Si vous souhaitez vous connecter en tant qu'utilisateur différent, vous devez d'abord vous déconnecter du portail AWS d'accès.

Réinitialisation de votre mot de passe utilisateur IAM Identity Center

Le portail AWS d'accès fournit aux utilisateurs d'IAM Identity Center un accès par authentification unique à tous les AWS comptes et applications cloud qui leur sont attribués via un portail Web. Le portail AWS d'accès est différent du AWS Management Console, qui est un ensemble de consoles de service permettant de gérer les AWS ressources.

Utilisez cette procédure pour réinitialiser votre mot de passe utilisateur IAM Identity Center pour le portail AWS d'accès. Pour en savoir plus sur les types d'utilisateurs, consultez le guide de Connexion à AWS l'utilisateur.

Considérations

La fonctionnalité de réinitialisation de votre mot de passe pour votre portail d' AWS accès n'est disponible que pour les utilisateurs des instances d'Identity Center qui utilisent le répertoire Identity Center ou AWS Managed Microsoft ADcomme source d'identité. Si votre utilisateur est connecté à un fournisseur d'identité externe ou à un AD Connector, les réinitialisations du mot de passe utilisateur doivent être effectuées depuis le fournisseur d'identité externe ou être connectéActive Directory.

- Si votre source d'identité est un annuaire IAM Identity Center, consultezExigences relatives aux mots de passe lors de la gestion des identités dans IAM Identity Center.
- Si votre source d'identité est une AWS Managed Microsoft AD, consultez la section Exigences relatives au mot de passe lors de la réinitialisation d'un mot de passe. AWS Managed Microsoft AD

Pour réinitialiser votre mot de passe pour AWS accéder au portail d'accès

1. Ouvrez un navigateur Web et accédez à la page de connexion de votre portail AWS d'accès.

   Si vous n'avez pas l'URL de votre portail d' AWS accès, vérifiez vos e-mails. Vous devriez avoir reçu par e-mail une invitation à rejoindre AWS IAM Identity Center qui inclut une URL de connexion spécifique au portail d'accès. AWS Il se peut également que votre administrateur vous ait directement fourni un mot de passe à usage unique et l'URL du portail AWS d'accès. Si vous ne trouvez pas ces informations, demandez à votre administrateur de vous les envoyer.

Pour plus d'informations sur la connexion au portail AWS d'accès, voir Se connecter au portail AWS d'accès dans le guide de Connexion à AWS l'utilisateur.

2. Entrez votre nom d'utilisateur, puis choisissez Next.
3. Sous Mot de passe, choisissez Mot de passe oublié.

   Vérifiez votre nom d'utilisateur et entrez les caractères de l'image fournie pour confirmer que vous n'êtes pas un robot. Ensuite, sélectionnez Suivant. Vous devrez peut-être désactiver le logiciel de blocage des publicités si vous ne pouvez pas saisir de caractères.
4. Un message s'affiche pour confirmer qu'un e-mail de réinitialisation du mot de passe a été envoyé. Choisissez Continuer.
5. Vous recevrez un e-mail de la part du destinataire `no-reply@signin.aws` avec le sujet Réinitialisation du mot de passe demandée. Dans votre e-mail, choisissez Réinitialiser le mot de passe.
6. Sur la page Réinitialiser le mot de passe, vérifiez votre nom d'utilisateur, spécifiez un nouveau mot de passe pour le portail AWS d'accès, puis choisissez Définir un nouveau mot de passe.
7. Vous recevrez un e-mail de la part de l'expéditeur `no-reply@signin.aws` dont l'objet sera « Mot de passe mis à jour ».

> **Note**
>
> Un administrateur peut réinitialiser votre mot de passe soit en vous envoyant un e-mail contenant des instructions pour réinitialiser votre mot de passe, soit en générant un mot de passe à usage unique et en le partageant avec vous. Si vous êtes administrateur, consultezRéinitialisation du mot de passe utilisateur IAM Identity Center pour un utilisateur final.

Obtention des informations d'identification utilisateur d'IAM Identity Center pour les SDK AWS CLI ou AWS

Vous pouvez accéder aux AWS services par programmation à l'aide des kits de développement logiciel (SDK) AWS Command Line Interface ou des kits de développement AWS logiciel (SDK) avec les informations d'identification utilisateur d'IAM Identity Center. Cette rubrique décrit comment obtenir des informations d'identification temporaires pour un utilisateur dans IAM Identity Center.

Le portail AWS d'accès fournit aux utilisateurs d'IAM Identity Center un accès par authentification unique à leurs applications Comptes AWS et à celles du cloud. Une fois connecté au portail d' AWS accès en tant qu'utilisateur de l'IAM Identity Center, vous pouvez obtenir des informations d'identification temporaires. Vous pouvez ensuite utiliser les informations d'identification, également appelées informations d'identification utilisateur IAM Identity Center, dans le AWS CLI ou les AWS SDK pour accéder aux ressources d'un. Compte AWS

Si vous utilisez le AWS CLI pour accéder aux AWS services par programmation, vous pouvez utiliser les procédures décrites dans cette rubrique pour initier l'accès au. AWS CLI Pour plus d'informations à ce sujet AWS CLI, consultez le guide de AWS Command Line Interface l'utilisateur.

Si vous utilisez les AWS SDK pour accéder aux AWS services par programmation, le respect des procédures décrites dans cette rubrique permet également d'établir directement l'authentification des SDK. AWS Pour plus d'informations sur les AWS SDK, consultez le Guide de référence AWS des SDK et des outils.

> **Note**
>
> Les utilisateurs d'IAM Identity Center sont différents des utilisateurs d'IAM. Les utilisateurs IAM reçoivent des informations d'identification à long terme pour les AWS ressources. Les utilisateurs d'IAM Identity Center reçoivent des informations d'identification temporaires. Nous vous recommandons d'utiliser des informations d'identification temporaires comme meilleure pratique de sécurité pour accéder à votre compte, Comptes AWS car ces informations d'identification sont générées à chaque fois que vous vous connectez.

Prérequis

Pour obtenir des informations d'identification temporaires pour votre utilisateur IAM Identity Center, vous aurez besoin des éléments suivants :

- Un utilisateur du IAM Identity Center : vous allez vous connecter au portail AWS d'accès en tant qu'utilisateur. Vous ou votre administrateur pouvez créer cet utilisateur. Pour plus d'informations sur la façon d'activer IAM Identity Center et de créer un utilisateur IAM Identity Center, consultez. Démarrez avec les tâches courantes dans IAM Identity Center
- Accès utilisateur à un Compte AWS — Pour accorder à un utilisateur IAM Identity Center l'autorisation de récupérer ses informations d'identification temporaires, vous ou un administrateur devez attribuer à l'utilisateur IAM Identity Center un ensemble d'autorisations. Les ensembles

d'autorisations sont stockés dans IAM Identity Center et définissent le niveau d'accès d'un utilisateur d'IAM Identity Center à un. Compte AWS Si votre administrateur a créé l'utilisateur IAM Identity Center pour vous, demandez-lui d'ajouter cet accès pour vous. Pour plus d'informations, consultez Attribuer un accès utilisateur à Comptes AWS.

- AWS CLI installé — Pour utiliser les informations d'identification temporaires, vous devez installer le AWS CLI. Pour obtenir des instructions, consultez Installation ou mise à jour de la dernière version de l' AWS CLI dans le Guide de l'utilisateur de l'AWS CLI .

Considérations

Avant de terminer les étapes permettant d'obtenir des informations d'identification temporaires pour votre utilisateur IAM Identity Center, tenez compte des points suivants :

- IAM Identity Center crée des rôles IAM : lorsque vous assignez un utilisateur dans IAM Identity Center à un ensemble d'autorisations, IAM Identity Center crée un rôle IAM correspondant à partir du jeu d'autorisations. Les rôles IAM créés par des ensembles d'autorisations diffèrent des rôles IAM créés de la AWS Identity and Access Management manière suivante :
  - IAM Identity Center possède et sécurise les rôles créés par les ensembles d'autorisations. Seul IAM Identity Center peut modifier ces rôles.
  - Seuls les utilisateurs d'IAM Identity Center peuvent assumer les rôles correspondant aux ensembles d'autorisations qui leur ont été attribués. Vous ne pouvez pas attribuer d'accès aux ensembles d'autorisations aux utilisateurs IAM, aux utilisateurs fédérés IAM ou aux comptes de service.
  - Vous ne pouvez pas modifier une politique de confiance relative à ces rôles pour autoriser l'accès aux principaux en dehors d'IAM Identity Center.

  Pour plus d'informations sur la façon d'obtenir des informations d'identification temporaires pour un rôle que vous créez dans IAM, consultez la section Utilisation des informations d'identification de sécurité temporaires AWS CLI dans le guide de l'AWS Identity and Access Management utilisateur.
- Vous pouvez définir la durée de session pour les ensembles d'autorisations : une fois que vous vous êtes connecté au portail d' AWS accès, le jeu d'autorisations auquel votre utilisateur IAM Identity Center est attribué apparaît comme un rôle disponible. IAM Identity Center crée une session distincte pour ce rôle. Cette session peut durer de une à 12 heures, selon la durée de session configurée pour l'ensemble d'autorisations. La durée de session par défaut est d'une heure. Pour plus d'informations, consultez Définir la durée de la session.

Obtenir et actualiser les informations d'identification temporaires

Vous pouvez obtenir et actualiser les informations d'identification temporaires de votre utilisateur IAM Identity Center automatiquement ou manuellement.

Rubriques

Actualisation automatique des informations d'identification (recommandée)

L'actualisation automatique des informations d'identification utilise la norme Open ID Connect (OIDC) Device Code Authorization. Avec cette méthode, vous initiez l'accès directement à l'aide de la `aws configure sso` commande figurant dans le AWS CLI. Vous pouvez utiliser cette commande pour accéder automatiquement à tout rôle associé à un ensemble d'autorisations qui vous est attribué pour n'importe quel rôle Compte AWS.

Pour accéder au rôle créé pour votre utilisateur IAM Identity Center, exécutez la `aws configure sso` commande, puis autorisez-la AWS CLI depuis une fenêtre de navigateur. Tant que vous avez une session active sur le portail AWS d'accès, il récupère AWS CLI automatiquement les informations d'identification temporaires et les actualise automatiquement.

Pour plus d'informations, consultez la section Configurer votre profil avec le `aws configure sso wizard` dans le guide de AWS Command Line Interface l'utilisateur.

Pour obtenir des informations d'identification temporaires qui s'actualisent automatiquement

1. Connectez-vous au portail d' AWS accès à l'aide de l'URL de connexion spécifique fournie par votre administrateur. Si vous avez créé l'utilisateur IAM Identity Center, vous avez AWS envoyé une invitation par e-mail contenant votre URL de connexion. Pour plus d'informations, voir Se connecter au portail AWS d'accès dans le Guide de l'utilisateur de AWS connexion.
2. Dans l'onglet Comptes, recherchez les informations d'identification Compte AWS à partir desquelles vous souhaitez récupérer les informations d'identification. Lorsque vous choisissez le compte, le nom du compte, l'identifiant du compte et l'adresse e-mail associés au compte apparaissent.

> **Note**
>
> Si aucune autorisation n'est Comptes AWSrépertoriée, il est probable qu'aucun ensemble d'autorisations ne vous ait encore été attribué pour ce compte. Dans ce cas, contactez votre administrateur et demandez-lui d'ajouter cet accès pour vous. Pour plus d'informations, consultez Attribuer un accès utilisateur à Comptes AWS.

3. Sous le nom du compte, le jeu d'autorisations auquel votre utilisateur IAM Identity Center est attribué apparaît sous la forme d'un rôle disponible. Par exemple, si l'utilisateur de votre IAM Identity Center est affecté à l'ensemble d'PowerUserAccessautorisations pour le compte, le rôle apparaît dans le portail AWS d'accès sous PowerUserAccessla forme.
4. En fonction de l'option que vous avez choisie à côté du nom du rôle, choisissez les touches d'accès ou l'accès par ligne de commande ou par programmation.
5. Dans la boîte de dialogue Obtenir les informations d'identification, choisissez macOS et Linux, Windows ou PowerShell, selon le système d'exploitation sur lequel vous avez installé le AWS CLI.
6. Sous les informations d'identification du centre d'identitéAWS IAM (recommandé), vos `SSO Start URL` identifiants `SSO Region` sont affichés. Ces valeurs sont requises pour configurer à la fois un profil activé par IAM Identity Center et `sso-session` pour votre AWS CLI. Pour terminer cette configuration, suivez les instructions de la section Configurer votre profil `aws configure sso wizard` à l'aide du guide de l'AWS Command Line Interface utilisateur.

Continuez à utiliser le AWS CLI selon vos besoins Compte AWS jusqu'à ce que les informations d'identification aient expiré.

Actualisation manuelle des informations d'identification

Vous pouvez utiliser la méthode d'actualisation manuelle des informations d'identification pour obtenir des informations d'identification temporaires pour un rôle associé à un ensemble d'autorisations spécifique dans un domaine spécifique Compte AWS. Pour ce faire, vous devez copier et coller les commandes requises pour les informations d'identification temporaires. Avec cette méthode, vous devez actualiser les informations d'identification temporaires manuellement.

Vous pouvez exécuter des AWS CLI commandes jusqu'à ce que vos informations d'identification temporaires expirent.

Pour obtenir des informations d'identification que vous actualisez manuellement

1. Connectez-vous au portail d' AWS accès à l'aide de l'URL de connexion spécifique fournie par votre administrateur. Si vous avez créé l'utilisateur IAM Identity Center, vous avez AWS envoyé une invitation par e-mail contenant votre URL de connexion. Pour plus d'informations, voir Se connecter au portail AWS d'accès dans le Guide de l'utilisateur de AWS connexion.
2. Dans l'onglet Comptes, recherchez le nom du rôle IAM à Compte AWS partir duquel vous souhaitez récupérer les informations d'accès et développez-le pour afficher le nom du rôle IAM (par exemple Administrateur). En fonction de votre option à côté du nom du rôle IAM, choisissez les touches d'accès ou choisissez l'accès par ligne de commande ou par programmation.

   > **Note**
   >
   > Si aucune autorisation n'est Comptes AWSrépertoriée, il est probable qu'aucun ensemble d'autorisations ne vous ait encore été attribué pour ce compte. Dans ce cas, contactez votre administrateur et demandez-lui d'ajouter cet accès pour vous. Pour plus d'informations, consultez Attribuer un accès utilisateur à Comptes AWS.

3. Dans la boîte de dialogue Obtenir les informations d'identification, choisissez macOS et Linux, Windows ou PowerShell, selon le système d'exploitation sur lequel vous avez installé le AWS CLI.
4. Choisissez l'une des options suivantes :

   - Option 1 : définir les variables d' AWS environnement

     Choisissez cette option pour annuler tous les paramètres d'identification, y compris les paramètres des `credentials` fichiers et `config` des fichiers. Pour plus d'informations, reportez-vous à la section Variables d'environnement pour les configurer AWS CLI dans le Guide de AWS CLI l'utilisateur.

     Pour utiliser cette option, copiez les commandes dans votre presse-papiers, collez-les dans la fenêtre de votre AWS CLI terminal, puis appuyez sur Entrée pour définir les variables d'environnement requises.

   - Option 2 : ajouter un profil à votre fichier AWS d'informations d'identification

     Choisissez cette option pour exécuter des commandes avec différents ensembles d'informations d'identification.

Pour utiliser cette option, copiez les commandes dans votre presse-papiers, puis collez-les dans votre AWS `credentials` fichier partagé pour configurer un nouveau profil nommé. Pour plus d'informations, consultez la section Fichiers de configuration et d'informations d'identification partagés dans le Guide de référence AWS des SDK et des outils. Pour utiliser ces informations d'identification, spécifiez l'`--profile`option dans votre AWS CLI commande. Cela concerne tous les environnements qui utilisent le même fichier d'informations d'identification.

- Option 3 : utilisez des valeurs individuelles dans votre AWS service client

  Choisissez cette option pour accéder aux AWS ressources d'un client AWS de service. Pour plus d'informations, consultez la section Outils sur lesquels vous pouvez vous appuyer AWS.

  Pour utiliser cette option, copiez les valeurs dans votre presse-papiers, collez-les dans votre code et attribuez-les aux variables appropriées pour votre SDK. Pour plus d'informations, consultez la documentation de l'API de votre SDK spécifique.

Création de liens de raccourci vers des AWS Management Console destinations

Les liens de raccourci créés dans le portail AWS d'accès dirigent les utilisateurs d'IAM Identity Center vers une destination spécifique dans le AWS Management Console, avec un ensemble d'autorisations spécifique, et dans un autre. Compte AWS

Les liens de raccourci vous font gagner du temps, à vous et à vos collaborateurs. Au lieu de naviguer vers l'URL de destination souhaitée AWS Management Console (par exemple, une page d'instance de compartiment Amazon S3) via plusieurs pages, y compris le portail AWS d'accès, vous pouvez utiliser un lien de raccourci pour accéder automatiquement à la même destination.

Options de destination des liens de raccourci

Les liens de raccourci comportent trois options de destination, répertoriées ici par ordre de priorité :

- (Facultatif) Toute URL de destination AWS Management Console spécifiée dans le lien de raccourci. Par exemple, la page relative à l'instance du compartiment Amazon S3.
- (Facultatif) URL de l'état du relais configurée par l'administrateur pour l'ensemble d'autorisations en question. Pour plus d'informations sur le réglage de l'état du relais, consultezDéfinir l'état du relais.
- AWS Management Console maison. Destination par défaut si vous n'en spécifiez aucune.

> **Note**
>
> La navigation automatique vers une destination n'est réussie que lorsque vous êtes authentifié auprès d'IAM Identity Center et que les autorisations nécessaires sont attribuées pour le AWS compte et l'URL de destination.

Le portail AWS d'accès inclut un bouton Créer un raccourci qui vous permet de créer un lien de raccourci partageable. Si vous prévoyez de spécifier une URL de destination (première option de la liste précédente), vous pouvez copier l'URL dans un presse-papiers pour la partager.

Création d'un lien de raccourci dans le portail AWS d'accès

1. Lorsque vous êtes connecté au portail AWS d'accès, cliquez sur l'onglet Comptes, puis sur le bouton Créer un raccourci.
2. Dans la boîte de dialogue :

   a. Choisissez un Compte AWS en utilisant l'identifiant ou le nom du compte. Au fur et à mesure que vous tapez, un menu déroulant affiche les identifiants de compte correspondants et les noms auxquels vous pouvez accéder. Vous ne pouvez choisir qu'un compte auquel vous avez accès.

   b. Choisissez éventuellement un rôle IAM dans la liste déroulante. Il s'agit des ensembles d'autorisations qui vous sont attribués pour le compte sélectionné. Si vous omettez de sélectionner le rôle, les utilisateurs sont invités à en sélectionner un qui leur est attribué pour le compte choisi lorsqu'ils utilisent le lien de raccourci.

   > **Note**
   >
   > Vous ne pouvez pas accorder un nouvel accès à l'aide de liens de raccourci. Les liens de raccourci fonctionnent uniquement avec les ensembles d'autorisations déjà attribués à l'utilisateur. Si l'utilisateur ne dispose pas des ensembles d'autorisations nécessaires pour le compte et l'URL de destination, l'accès lui est refusé.

   c. Entrez éventuellement l'URL de destination du portail d' AWS accès. Si vous omettez de saisir une URL, la destination est automatiquement déterminée lors de l'utilisation du lien de raccourci, en fonction des options de destination du lien de raccourci mentionnées précédemment.

d. Votre lien de raccourci est généré en bas de la boîte de dialogue, en fonction de vos entrées. Cliquez sur le bouton Copier l'URL. Vous pouvez désormais créer un signet avec le lien de raccourci copié ou le partager avec vos collaborateurs qui ont accès au même compte avec le même ensemble d'autorisations ou un autre ensemble d'autorisations suffisant.

Création de liens de AWS Management Console raccourci sécurisés avec encodage d'URL

Toutes les valeurs des paramètres de l'URL, y compris l'ID du compte, le nom de l'ensemble d'autorisations et l'URL de destination, doivent être codées en URL.

Les liens de raccourci étendent l'URL du portail d' AWS accès avec le chemin suivant :

```
/#/console?
account_id=[account_ID]&role_name=[permission_set_name]&destination=[destination
```

L'URL complète de la AWS partition classique suit le modèle suivant :

```
https://[your_subdomain].awsapps.com/start/#/console?
account_id=[account_ID]&role_name=[permission_set_name]&destination=[destination
```

Voici un exemple de lien de raccourci qui permet à un utilisateur de se connecter à un compte `123456789012` avec l'ensemble d'`S3FullAccess`autorisations et d'accéder à la page d'accueil de la console S3 :

- `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`

Enregistrement d'un appareil pour le MFA

Utilisez la procédure suivante dans le portail AWS d'accès pour enregistrer votre nouvel appareil pour l'authentification multifactorielle (MFA).

> **Note**
>
> Nous vous recommandons de télécharger d'abord l'application Authenticator appropriée sur votre appareil avant de commencer les étapes de cette procédure. Pour obtenir la liste des applications que vous pouvez utiliser pour les appareils MFA, consultez. Applications d'authentification virtuelle

Pour enregistrer votre appareil afin de l'utiliser avec le MFA

1. Connectez-vous à votre portail AWS d'accès. Pour plus d'informations, consultez Connexion au portail d' AWS accès.
2. En haut à droite de la page, sélectionnez les appareils MFA.
3. Sur la page des appareils d'authentification multifactorielle (MFA), choisissez Enregistrer un appareil.

   > **Note**
   >
   > Si l'option Enregistrer un appareil MFA est grisée, contactez votre administrateur pour obtenir de l'aide pour enregistrer votre appareil.

4. Sur la page Enregistrer un appareil MFA, sélectionnez l'un des types de périphériques MFA suivants et suivez les instructions :

   - Application Authenticator
     1. Sur la page Configurer l'application d'authentification, vous remarquerez peut-être des informations de configuration pour le nouveau dispositif MFA, notamment un code QR graphique. Le graphique est une représentation de la clé secrète qui peut être saisie manuellement sur les appareils qui ne prennent pas en charge les codes QR.
     2. À l'aide du périphérique MFA physique, procédez comme suit :
        a. Ouvrez une application d'authentification MFA compatible. Pour obtenir la liste des applications testées que vous pouvez utiliser avec les appareils MFA, consultez. Applications d'authentification virtuelle Si l'application MFA prend en charge plusieurs comptes (plusieurs appareils MFA), choisissez l'option permettant de créer un nouveau compte (un nouvel appareil MFA).
        b. Déterminez si l'application MFA prend en charge les codes QR, puis effectuez l'une des opérations suivantes sur la page Configurer l'application d'authentification :

i. Choisissez Afficher le code QR, puis utilisez l'application pour scanner le code QR. Par exemple, vous pouvez choisir l'icône de l'appareil photo ou une option similaire à Scanner le code. Utilisez ensuite l'appareil photo de l'appareil pour scanner le code.

ii. Choisissez Afficher la clé secrète, puis entrez cette clé secrète dans votre application MFA.

> **Important**
>
> Lorsque vous configurez un dispositif MFA pour IAM Identity Center, nous vous recommandons d'enregistrer une copie du code QR ou de la clé secrète dans un endroit sûr. Cela peut être utile si vous perdez le téléphone ou si vous devez réinstaller l'application d'authentification MFA. Si l'une de ces situations se produit, vous pouvez rapidement reconfigurer l'application pour qu'elle utilise la même configuration MFA.

3. Sur la page Configurer l'application d'authentification, sous Code d'authentification, entrez le mot de passe à usage unique qui apparaît actuellement sur le dispositif MFA physique.

> **Important**
>
> Envoyez votre demande immédiatement après avoir généré le code. Si vous générez le code puis attendez trop longtemps pour envoyer la demande, le dispositif MFA est correctement associé à votre utilisateur, mais le dispositif MFA n'est pas synchronisé. En effet, les TOTP (Time-based One-Time Passwords ou mots de passe à usage unique à durée limitée) expirent après une courte période. Dans ce cas, vous pouvez synchroniser à nouveau l'appareil.

4. Choisissez Assign MFA (Affecter le MFA). Le dispositif MFA peut désormais commencer à générer des mots de passe à usage unique et est maintenant prêt à être utilisé avec. AWS

- Clé de sécurité ou authentificateur intégré

1. Sur la page Enregistrer la clé de sécurité de votre utilisateur, suivez les instructions fournies par votre navigateur ou votre plateforme.

> **Note**
>
> L'expérience varie en fonction du navigateur ou de la plateforme. Une fois votre appareil enregistré avec succès, vous pouvez associer un nom d'affichage convivial à l'appareil que vous venez d'inscrire. Pour modifier le nom, choisissez Renommer, entrez le nouveau nom, puis cliquez sur Enregistrer.

Personnalisation de l'URL du portail AWS d'accès

Par défaut, vous pouvez accéder au portail AWS d'accès en utilisant une URL au format suivant :`d-xxxxxxxxxx.awsapps.com/start`. Vous pouvez personnaliser l'URL comme suit :`your_subdomain.awsapps.com/start`.

> **Important**
>
> Si vous modifiez l'URL du portail AWS d'accès, vous ne pourrez pas la modifier ultérieurement.

Pour personnaliser votre URL

1. Ouvrez la AWS IAM Identity Center console à l'adresse https://console.aws.amazon.com/singlesignon/.
2. Dans la console IAM Identity Center, choisissez Dashboard dans le volet de navigation et recherchez la section récapitulative des paramètres.
3. Cliquez sur le bouton Personnaliser situé sous l'URL de votre portail AWS d'accès.

   > **Note**
   >
   > Si le bouton Personnaliser ne s'affiche pas, cela signifie que le portail AWS d'accès a déjà été personnalisé. La personnalisation de l'URL du portail d' AWS accès est une opération unique irréversible.

4. Entrez le nom de sous-domaine souhaité et choisissez Enregistrer.

Vous pouvez désormais vous connecter à la AWS console via votre portail AWS d'accès à l'aide de votre URL personnalisée.

Authentification multifactorielle pour les utilisateurs d'Identity Center

L'authentification multifactorielle (MFA) fournit un moyen simple et sécurisé d'ajouter une couche de protection supplémentaire en plus du mécanisme d'authentification par défaut du nom d'utilisateur et du mot de passe.

Lorsque les administrateurs activent le MFA, les utilisateurs doivent se connecter au portail d'AWSaccès en respectant deux critères :

- Leurs nom d'utilisateur et mot de passe. C'est le premier facteur et les utilisateurs le savent.
- Il s'agit d'un code, d'une clé de sécurité ou de données biométriques. Il s'agit du deuxième facteur et c'est quelque chose que les utilisateurs possèdent (possession) ou sont (biométrie). Le deuxième facteur peut être soit un code d'authentification généré par son appareil mobile, soit une clé de sécurité connectée à son ordinateur, soit le scan biométrique de l'utilisateur.

Ensemble, ces multiples facteurs renforcent la sécurité en empêchant tout accès non autorisé à vos AWS ressources à moins qu'un défi MFA valide n'ait été relevé avec succès.

Chaque utilisateur peut enregistrer jusqu'à deux applications d'authentification virtuelles, qui sont des applications d'authentification par mot de passe à usage unique installées sur votre appareil mobile ou votre tablette, et six authentificateurs FIDO, qui incluent des authentificateurs intégrés et des clés de sécurité, pour un total de huit appareils MFA. En savoir plus sur Types de MFA disponibles pour IAM Identity Center.

> **Important**
>
> Pour des raisons de sécurité, nous vous recommandons vivement d'activer la MFA.

Rubriques

Types de MFA disponibles pour IAM Identity Center

L'authentification multifactorielle (MFA) est un mécanisme simple et efficace pour renforcer la sécurité de vos utilisateurs. Le premier facteur d'un utilisateur, son mot de passe, est un secret qu'il mémorise, également appelé facteur de connaissance. Les autres facteurs peuvent être des facteurs liés à la possession (quelque chose que vous possédez, comme une clé de sécurité) ou des facteurs inhérents (quelque chose que vous êtes, comme un scan biométrique). Nous vous recommandons vivement de configurer le MFA pour ajouter un niveau de sécurité supplémentaire à votre compte.

Le MFA IAM Identity Center prend en charge les types d'appareils suivants. Tous les types de MFA sont pris en charge à la fois pour l'accès à la console via un navigateur et pour l'utilisation de la AWS CLI version v2 avec IAM Identity Center.

- Authentificateurs FIDO2, y compris les authentificateurs intégrés et les clés de sécurité
- Applications d'authentification virtuelle
- Votre propre RAYON MFA implémentation connectée via AWS Managed Microsoft AD

Un utilisateur peut avoir jusqu'à huit appareils MFA, dont deux applications d'authentification virtuelle et six authentificateurs FIDO, enregistrés sur un seul compte. Vous pouvez également configurer les paramètres d'activation de l'authentification multifacteur pour exiger l'authentification multifacteur chaque fois que vos utilisateurs se connectent ou pour activer les appareils fiables qui ne nécessitent pas l'authentification multifacteur à chaque connexion. Pour plus d'informations sur la configuration des types MFA pour vos utilisateurs, consultez Choisissez les types de MFA et. Configurer l'application des dispositifs MFA

Authentificateurs FIDO2

FIDO2 est une norme qui inclut le CTAP2 WebAuthnet qui est basée sur la cryptographie à clé publique. Les informations d'identification FIDO résistent au hameçonnage car elles sont uniques au site Web sur lequel elles ont été créées, par exemple. AWS

AWSprend en charge les deux formats les plus courants pour les authentificateurs FIDO : les authentificateurs intégrés et les clés de sécurité. Voir ci-dessous pour plus d'informations sur les types les plus courants d'authentificateurs FIDO.

Rubriques

- Authentificateurs intégrés

- Clés de sécurité
- Gestionnaires de mots de passe, fournisseurs de clés d'accès et autres authentificateurs FIDO

Authentificateurs intégrés

De nombreux ordinateurs et téléphones portables modernes sont dotés d'authentificateurs intégrés, tels que TouchID sur Macbook ou un appareil photo compatible avec Windows Hello. Si votre appareil est doté d'un authentificateur intégré compatible avec Fido, vous pouvez utiliser votre empreinte digitale, votre visage ou le code PIN de votre appareil comme deuxième facteur.

Clés de sécurité

Les clés de sécurité sont des authentificateurs matériels externes compatibles avec FIDO que vous pouvez acheter et connecter à votre appareil via USB, BLE ou NFC. Lorsque le MFA vous est demandé, il vous suffit de faire un geste avec le capteur de la touche. Parmi les clés de sécurité, citons les clés feitiennes, YubiKeys et les clés de sécurité les plus courantes créent des informations d'identification FIDO liées à l'appareil. Pour une liste de toutes les clés de sécurité certifiées FIDO, consultez la section Produits certifiés FIDO.

Gestionnaires de mots de passe, fournisseurs de clés d'accès et autres authentificateurs FIDO

Plusieurs fournisseurs tiers prennent en charge l'authentification FIDO dans les applications mobiles, sous forme de fonctionnalités dans les gestionnaires de mots de passe, les cartes à puce dotées d'un mode FIDO et d'autres formats. Ces appareils compatibles avec FIDO peuvent fonctionner avec IAM Identity Center, mais nous vous recommandons de tester vous-même un authentificateur FIDO avant d'activer cette option pour le MFA.

> **Note**
>
> Certains authentificateurs FIDO peuvent créer des informations d'identification FIDO détectables appelées clés d'accès. Les clés d'accès peuvent être liées à l'appareil qui les a créées, ou elles peuvent être synchronisées et sauvegardées dans un cloud. Par exemple, vous pouvez enregistrer une clé d'accès à l'aide d'Apple Touch ID sur un Macbook compatible, puis vous connecter à un site depuis un ordinateur portable Windows à l'aide de Google Chrome avec votre clé d'accès dans iCloud en suivant les instructions qui s'affichent à l'écran lors de la connexion. Pour plus d'informations sur les appareils compatibles avec les clés d'accès synchronisées et sur l'interopérabilité actuelle des clés d'accès entre les systèmes d'exploitation et les navigateurs, consultez la section Support des appareils sur

passkeys.dev, une ressource gérée par l'Alliance FIDO et le World Wide Web Consortium (W3C).

Applications d'authentification virtuelle

Les applications d'authentification sont essentiellement des authentificateurs tiers basés sur un mot de passe à usage unique (OTP). Vous pouvez utiliser une application d'authentification installée sur votre appareil mobile ou votre tablette en tant qu'appareil MFA autorisé. L'application d'authentification tierce doit être conforme à la RFC 6238, qui est un algorithme de mot de passe à usage unique (TOTP) basé sur des normes et basé sur le temps capable de générer des codes d'authentification à six chiffres.

Lorsqu'ils sont invités à saisir le MFA, les utilisateurs doivent saisir un code valide provenant de leur application d'authentification dans la zone de saisie présentée. Chaque dispositif MFA attribué à un utilisateur doit être unique. Deux applications d'authentification peuvent être enregistrées pour un utilisateur donné.

Applications d'authentification testées

Toute application conforme au TOTP fonctionnera avec le MFA d'IAM Identity Center. Le tableau suivant répertorie les applications d'authentification tierces les plus connues parmi lesquelles choisir.

Système d'exploitation	Application d'authentification testée
Android	Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator
iOS	Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator

RAYON MFA

Le Remote Authentication Dial-In User Service (RADIUS) est un protocole client-serveur standard qui assure l'authentification, l'autorisation et la gestion de la comptabilité afin que les utilisateurs puissent se connecter aux services réseau. AWS Directory Serviceinclut un client RADIUS qui se connecte au serveur RADIUS sur lequel vous avez implémenté votre solution MFA. Pour plus d'informations, voir Activer l'authentification multifactorielle pour AWS Managed Microsoft AD.

Vous pouvez utiliser RADIUS MFA ou MFA dans IAM Identity Center pour les connexions des utilisateurs au portail utilisateur, mais pas les deux. La MFA dans IAM Identity Center est une alternative à la MFA RADIUS dans les cas où vous souhaitez une authentification AWS native à deux facteurs pour accéder au portail.

Lorsque vous activez l'authentification multifacteur dans IAM Identity Center, vos utilisateurs ont besoin d'un appareil MFA pour se connecter au portail d'accès. AWS Si vous avez déjà utilisé RADIUS MFA, l'activation de la MFA dans IAM Identity Center remplace efficacement la MFA RADIUS pour les utilisateurs qui se connectent au portail d'accès. AWS Cependant, le MFA RADIUS continue de poser des problèmes aux utilisateurs lorsqu'ils se connectent à toutes les autres applications compatiblesAWS Directory Service, telles qu'Amazon. WorkDocs

Si votre MFA est désactivé sur la console IAM Identity Center et que vous avez configuré RADIUS MFA avec, AWS Directory Service RADIUS MFA régit la connexion au portail d'accès. AWS Cela signifie qu'IAM Identity Center revient à la configuration RADIUS MFA si la MFA est désactivée.

Configuration de la MFA

Les rubriques suivantes fournissent des instructions pour configurer les appareils MFA dans IAM Identity Center.

Rubriques

Considérations à prendre en compte avant d'activer la MFA dans IAM Identity Center

Avant d'activer la MFA, tenez compte des points suivants :

- Les utilisateurs sont invités à enregistrer plusieurs authentificateurs de sauvegarde pour tous les types de MFA activés. Cette pratique permet d'éviter la perte d'accès en cas de panne ou d'égarement d'un dispositif MFA.
- Ne choisissez pas l'option Exiger qu'ils fournissent un mot de passe à usage unique envoyé par e-mail si vos utilisateurs doivent se connecter au portail AWS d'accès pour accéder à leur

courrier électronique. Par exemple, vos utilisateurs peuvent utiliser Microsoft 365 le portail AWS d'accès pour lire leurs e-mails. Dans ce cas, les utilisateurs ne pourront pas récupérer le code de vérification et ne pourront pas se connecter au portail AWS d'accès. Pour plus d'informations, consultez Configurer l'application des dispositifs MFA.

- Si vous utilisez déjà le protocole RADIUS MFA que vous avez configuréAWS Directory Service, vous n'avez pas besoin d'activer le MFA dans IAM Identity Center. Le MFA dans IAM Identity Center est une alternative au MFA RADIUS pour les Microsoft Active Directory utilisateurs d'IAM Identity Center. Pour plus d'informations, consultez RAYON MFA.
- Vous pouvez utiliser les fonctionnalités MFA dans IAM Identity Center lorsque votre source d'identité est configurée avec le magasin d'identités d'IAM Identity Center, ou AWS Managed Microsoft AD AD Connector. Le MFA dans IAM Identity Center n'est actuellement pas pris en charge pour les fournisseurs d'identité externes.

Activer le MFA dans IAM Identity Center

Vous pouvez activer un accès sécurisé au portail d'AWSaccès, aux applications intégrées d'IAM Identity Center et AWS CLI en activant l'authentification multifactorielle (MFA).

Rubriques

- Inviter les utilisateurs à utiliser le MFA
- Désactiver le MFA pour votre répertoire IAM Identity Center

Inviter les utilisateurs à utiliser le MFA

Procédez comme suit pour activer le MFA dans la console IAM Identity Center. Avant de commencer, nous vous recommandons de comprendre leTypes de MFA disponibles pour IAM Identity Center.

> **Note**
>
> Si vous utilisez un IdP externe, la section Authentification multifactorielle ne sera pas disponible. Votre IdP externe gère les paramètres MFA, plutôt que IAM Identity Center les gère.

Pour activer le MFA

1. Ouvrez la console IAM Identity Center.

2. Dans le panneau de navigation de gauche, choisissez Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Authentification.
4. Dans la section Authentification multifactorielle, choisissez Configurer.
5. Sur la page Configurer l'authentification multifactorielle, sous Inviter les utilisateurs à utiliser la MFA, choisissez l'un des modes d'authentification suivants en fonction du niveau de sécurité dont votre entreprise a besoin :

   - Uniquement lorsque leur contexte de connexion change (sensible au contexte)

     Dans ce mode (par défaut), IAM Identity Center offre aux utilisateurs la possibilité de faire confiance à leur appareil lors de la connexion. Une fois qu'un utilisateur indique qu'il souhaite faire confiance à un appareil, IAM Identity Center lui demande une seule fois de saisir le MFA et analyse le contexte de connexion (tel que l'appareil, le navigateur et l'emplacement) pour les connexions ultérieures de l'utilisateur. Pour les connexions suivantes, IAM Identity Center détermine si l'utilisateur se connecte avec un contexte précédemment approuvé. Si le contexte de connexion de l'utilisateur change, IAM Identity Center l'invite à saisir le MFA en plus de son adresse e-mail et de son mot de passe.

     Ce mode facilite l'utilisation des utilisateurs qui se connectent fréquemment depuis leur lieu de travail, de sorte qu'ils n'ont pas besoin de compléter le MFA à chaque connexion. Ils ne sont invités à utiliser le MFA que si leur contexte de connexion change.
   - Chaque fois qu'ils se connectent (toujours activé)

     Dans ce mode, IAM Identity Center exige que les utilisateurs possédant un appareil MFA enregistré soient invités à chaque fois qu'ils se connectent. Vous devez utiliser ce mode si vous avez des politiques organisationnelles ou de conformité qui obligent vos utilisateurs à effectuer le MFA chaque fois qu'ils se connectent au portail d'AWSaccès. Par exemple, la norme PCI DSS recommande vivement l'authentification MFA lors de chaque connexion afin d'accéder aux applications qui prennent en charge les transactions de paiement à haut risque.
   - Jamais (désactivé)

     Dans ce mode, tous les utilisateurs se connectent uniquement avec leur nom d'utilisateur et leur mot de passe standard. Le choix de cette option désactive le MFA d'IAM Identity Center.

     > **Note**
     >
     > Si vous utilisez déjà RADIUS MFA avec AWS Directory Service et que vous souhaitez continuer à l'utiliser comme type de MFA par défaut, vous pouvez laisser le mode

d'authentification désactivé pour contourner les fonctionnalités MFA dans IAM Identity Center. Le passage du mode désactivé au mode contextuel ou permanent remplacera les paramètres MFA RADIUS existants. Pour plus d'informations, consultez RAYON MFA.

6. Choisissez Enregistrer les modifications.

Rubriques connexes

- Choisissez les types de MFA
- Configurer l'application des dispositifs MFA
- Autoriser les utilisateurs à enregistrer leurs propres appareils MFA

Désactiver le MFA pour votre répertoire IAM Identity Center

Lorsque vous désactivez l'authentification multifactorielle (MFA) pour votre annuaire IAM Identity Center, les utilisateurs ne peuvent se connecter qu'avec leur nom d'utilisateur et leur mot de passe standard. Bien que l'authentification MFA soit désactivée pour votre annuaire Identity Center pour les utilisateurs, vous ne pouvez pas gérer les appareils MFA dans leurs informations d'utilisateur, et les utilisateurs du répertoire Identity Center ne peuvent pas gérer les appareils MFA depuis le portail d'accès. AWS

Pour désactiver le MFA pour votre répertoire IAM Identity Center

Important

Les instructions de cette section s'appliquent à AWS IAM Identity Center. Ils ne s'appliquent pas à AWS Identity and Access Management(IAM). Les utilisateurs, les groupes et les informations d'identification utilisateur d'IAM Identity Center sont différents des informations d'identification des utilisateurs, des groupes et des utilisateurs IAM. Si vous recherchez des instructions sur la désactivation de l'authentification multifacteur pour les utilisateurs d'IAM, consultez la section Désactivation des appareils MFA dans le guide de l'utilisateur. AWS Identity and Access Management

1. Ouvrez la console IAM Identity Center.
2. Dans le panneau de navigation de gauche, choisissez Paramètres.

3. Sur la page Paramètres, choisissez l'onglet Authentification.
4. Dans la section Authentification multifactorielle, choisissez Configurer.
5. Sur la page Configurer l'authentification multifactorielle, dans la section Inviter les utilisateurs à utiliser l'authentification MFA, cliquez sur le bouton radio Jamais (désactivé).
6. Sélectionnez Enregistrer les modifications.

Choisissez les types de MFA

Utilisez la procédure suivante pour choisir les types d'appareils avec lesquels vos utilisateurs peuvent s'authentifier lorsqu'ils sont invités à saisir le MFA sur AWS le portail d'accès.

Pour configurer les types de MFA pour vos utilisateurs

1. Ouvrez la console IAM Identity Center.
2. Dans le panneau de navigation de gauche, choisissez Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Authentification.
4. Dans la section Authentification multifactorielle, choisissez Configurer.
5. Sur la page Configurer l'authentification multifactorielle, sous Les utilisateurs peuvent s'authentifier avec ces types de MFA, choisissez l'un des types d'authentification MFA suivants en fonction des besoins de votre entreprise. Pour plus d'informations, consultez Types de MFA disponibles pour IAM Identity Center.
   - Authentificateurs FIDO2, y compris les authentificateurs intégrés et les clés de sécurité
   - Applications d'authentification virtuelle
6. Sélectionnez Enregistrer les modifications.

Configurer l'application des dispositifs MFA

Utilisez la procédure suivante pour déterminer si vos utilisateurs doivent disposer d'un dispositif MFA enregistré lorsqu'ils se connectent au portail d'AWSaccès.

Pour configurer l'application des dispositifs MFA pour vos utilisateurs

1. Ouvrez la console IAM Identity Center.
2. Dans le panneau de navigation de gauche, choisissez Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Authentification.

4. Dans la section Authentification multifactorielle, choisissez Configurer.
5. Sur la page Configurer l'authentification multifactorielle, sous Si un utilisateur ne possède pas encore d'appareil MFA enregistré, choisissez l'une des options suivantes en fonction des besoins de votre entreprise :

   - Demandez-leur d'enregistrer un appareil MFA lors de la connexion

     Il s'agit du paramètre par défaut lorsque vous configurez pour la première fois le MFA pour IAM Identity Center. Utilisez cette option lorsque vous souhaitez demander aux utilisateurs qui ne possèdent pas encore d'appareil MFA enregistré d'inscrire eux-mêmes un appareil lors de la connexion après une authentification par mot de passe réussie. Cela vous permet de sécuriser les AWS environnements de votre entreprise grâce à la MFA sans avoir à inscrire et à distribuer des dispositifs d'authentification individuels à vos utilisateurs. Lors de l'auto-inscription, vos utilisateurs peuvent enregistrer n'importe quel appareil parmi les appareils disponibles que Types de MFA disponibles pour IAM Identity Center vous avez précédemment activés. Une fois l'enregistrement terminé, les utilisateurs ont la possibilité de donner un nom convivial à leur appareil MFA nouvellement inscrit, après quoi IAM Identity Center redirige l'utilisateur vers sa destination d'origine. En cas de perte ou de vol de l'appareil de l'utilisateur, vous pouvez simplement le supprimer de son compte, et IAM Identity Center demandera à l'utilisateur d'enregistrer lui-même un nouvel appareil lors de sa prochaine connexion.
   - Demandez-leur de fournir un mot de passe à usage unique envoyé par e-mail pour se connecter

     Utilisez cette option lorsque vous souhaitez que des codes de vérification soient envoyés aux utilisateurs par e-mail. Étant donné que le courrier électronique n'est pas lié à un appareil spécifique, cette option ne répond pas aux normes de l'industrie en matière d'authentification multifactorielle. Mais cela améliore la sécurité par rapport au simple fait d'avoir un mot de passe. La vérification par e-mail ne sera demandée que si l'utilisateur n'a pas enregistré d'appareil MFA. Si la méthode d'authentification sensible au contexte a été activée, l'utilisateur aura la possibilité de marquer l'appareil sur lequel il reçoit l'e-mail comme étant fiable. Par la suite, ils ne seront pas tenus de vérifier un code e-mail lors de futures connexions à partir de cette combinaison d'appareil, de navigateur et d'adresse IP.

     > **Note**
     >
     > Si vous utilisez Active Directory comme source d'identité activée par votre IAM Identity Center, l'adresse e-mail sera toujours basée sur l'`email`attribut Active Directory.

Les mappages d'attributs Active Directory personnalisés ne remplaceront pas ce comportement.

- Bloquer leur connexion

  Utilisez l'option Bloquer leur connexion lorsque vous souhaitez obliger chaque utilisateur à utiliser le MFA avant qu'il ne puisse se connecter. AWS

  > **Important**
  >
  > Si votre méthode d'authentification est configurée en fonction du contexte, un utilisateur peut cocher la case Ceci est un appareil fiable sur la page de connexion. Dans ce cas, cet utilisateur ne sera pas invité à utiliser le MFA même si le paramètre Bloquer sa connexion est activé. Si vous souhaitez que ces utilisateurs soient invités, remplacez votre méthode d'authentification par Always On.

- Autorisez-les à se connecter

  Utilisez cette option pour indiquer que les appareils MFA ne sont pas nécessaires pour que vos utilisateurs puissent se connecter au portail d'AWSaccès. Les utilisateurs qui ont choisi d'enregistrer des appareils MFA seront toujours invités à le faire.

6. Sélectionnez Enregistrer les modifications.

Autoriser les utilisateurs à enregistrer leurs propres appareils MFA

Suivez la procédure ci-dessous pour permettre à vos utilisateurs d'enregistrer eux-mêmes leurs propres appareils MFA.

Pour permettre aux utilisateurs d'enregistrer leurs propres appareils MFA

1. Ouvrez la console IAM Identity Center.
2. Dans le panneau de navigation de gauche, choisissez Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Authentification.
4. Dans la section Authentification multifactorielle, choisissez Configurer.
5. Sur la page Configurer l'authentification multifactorielle, sous Qui peut gérer les appareils MFA, choisissez Les utilisateurs peuvent ajouter et gérer leurs propres appareils MFA.
6. Sélectionnez Enregistrer les modifications.

> **Note**
>
> Après avoir configuré l'auto-enregistrement pour vos utilisateurs, vous souhaiterez peut-être leur envoyer un lien vers la procédureEnregistrement d'un appareil pour le MFA. Cette rubrique fournit des instructions sur la façon de configurer leurs propres dispositifs MFA.

Gérer les appareils MFA dans IAM Identity Center

Les rubriques suivantes fournissent des instructions pour gérer les appareils MFA dans IAM Identity Center.

Rubriques

- Enregistrer un appareil MFA
- Gérer le dispositif MFA d'un utilisateur

Enregistrer un appareil MFA

Utilisez la procédure suivante pour configurer un nouveau dispositif MFA auquel un utilisateur spécifique pourra accéder dans la console IAM Identity Center. Vous devez avoir un accès physique au dispositif MFA de l'utilisateur pour pouvoir l'enregistrer. Par exemple, si vous configurez l'authentification multifacteur pour un utilisateur qui utilisera un appareil MFA exécuté sur un smartphone, vous aurez besoin d'un accès physique au smartphone pour terminer le processus d'enregistrement. Vous pouvez également autoriser les utilisateurs à configurer et à gérer leurs propres appareils MFA. Pour plus d'informations, consultez Autoriser les utilisateurs à enregistrer leurs propres appareils MFA.

Pour enregistrer un appareil MFA

1. Ouvrez la console IAM Identity Center.
2. Dans le volet de navigation de gauche, choisissez Utilisateurs. Choisissez un utilisateur dans la liste. Ne cochez pas la case à côté de l'utilisateur pour cette étape.
3. Sur la page des informations utilisateur, choisissez l'onglet Appareils MFA, puis sélectionnez Enregistrer un appareil MFA.
4. Sur la page Enregistrer un appareil MFA, sélectionnez l'un des types de périphériques MFA suivants et suivez les instructions :

- Application Authenticator

1. Sur la page Configurer l'application d'authentification, IAM Identity Center affiche les informations de configuration du nouveau dispositif MFA, notamment un code QR graphique. Le graphique est une représentation de la clé secrète qui peut être saisie manuellement sur les appareils qui ne prennent pas en charge les codes QR.
2. À l'aide du périphérique MFA physique, procédez comme suit :

   a. Ouvrez une application d'authentification MFA compatible. Pour obtenir la liste des applications testées que vous pouvez utiliser avec les appareils MFA, consultez. Applications d'authentification virtuelle Si l'application MFA prend en charge plusieurs comptes (plusieurs appareils MFA), choisissez l'option permettant de créer un nouveau compte (un nouvel appareil MFA).

   b. Déterminez si l'application MFA prend en charge les codes QR, puis effectuez l'une des opérations suivantes sur la page Configurer l'application d'authentification :

      i. Choisissez Afficher le code QR, puis utilisez l'application pour scanner le code QR. Par exemple, vous pouvez choisir l'icône de l'appareil photo ou une option similaire à Scanner le code. Utilisez ensuite l'appareil photo de l'appareil pour scanner le code.

      ii. Choisissez Afficher la clé secrète, puis saisissez cette clé secrète dans votre application MFA.

      > **Important**
      >
      > Lorsque vous configurez un dispositif MFA pour IAM Identity Center, nous vous recommandons d'enregistrer une copie du code QR ou de la clé secrète dans un endroit sûr. Cela peut être utile si l'utilisateur désigné perd le téléphone ou doit réinstaller l'application d'authentification MFA. Si l'une de ces situations se produit, vous pouvez rapidement reconfigurer l'application pour qu'elle utilise la même configuration MFA. Cela évite à l'utilisateur de créer un nouveau dispositif MFA dans IAM Identity Center.

3. Sur la page Configurer l'application d'authentification, sous Code d'authentification, saisissez le mot de passe à usage unique qui apparaît actuellement sur le dispositif MFA physique.

> **Important**
>
> Envoyez votre demande immédiatement après avoir généré le code. Si vous générez le code puis attendez trop longtemps pour soumettre la demande, le dispositif MFA est correctement associé à l'utilisateur. Mais le dispositif MFA n'est pas synchronisé. En effet, les TOTP (Time-based One-Time Passwords ou mots de passe à usage unique à durée limitée) expirent après une courte période. Dans ce cas, vous pouvez resynchroniser le dispositif.

4. Choisissez Assign MFA (Affecter le MFA). Le dispositif MFA peut désormais commencer à générer des mots de passe à usage unique et est maintenant prêt à être utilisé avec. AWS

- Clé de sécurité

1. Sur la page Enregistrer la clé de sécurité de votre utilisateur, suivez les instructions fournies par votre navigateur ou votre plateforme.

> **Note**
>
> L'expérience ici varie en fonction des différents systèmes d'exploitation et navigateurs. Veuillez donc suivre les instructions affichées par votre navigateur ou votre plateforme. Une fois que l'appareil de votre utilisateur a été enregistré avec succès, vous aurez la possibilité d'associer un nom d'affichage convivial à l'appareil nouvellement inscrit de votre utilisateur. Si vous souhaitez modifier cela, choisissez Renommer, entrez le nouveau nom, puis cliquez sur Enregistrer. Si vous avez activé l'option permettant aux utilisateurs de gérer leurs propres appareils, l'utilisateur verra ce nom convivial sur le portail AWS d'accès.

Gérer le dispositif MFA d'un utilisateur

Utilisez les procédures suivantes lorsque vous devez renommer ou supprimer le dispositif MFA d'un utilisateur.

Pour renommer un appareil MFA

1. Ouvrez la console IAM Identity Center.

2. Dans le volet de navigation de gauche, choisissez Utilisateurs. Choisissez l'utilisateur dans la liste. Ne cochez pas la case à côté de l'utilisateur pour cette étape.
3. Sur la page des informations utilisateur, choisissez l'onglet Appareils MFA, sélectionnez l'appareil, puis choisissez Renommer.
4. Lorsque vous y êtes invité, entrez le nouveau nom, puis choisissez Renommer.

Pour supprimer un appareil MFA

1. Ouvrez la console IAM Identity Center.
2. Dans le volet de navigation de gauche, choisissez Utilisateurs. Choisissez l'utilisateur dans la liste.
3. Sur la page des informations utilisateur, choisissez l'onglet Appareils MFA, sélectionnez l'appareil, puis choisissez Supprimer.
4. Pour confirmer, tapez DELETE, puis sélectionnez Supprimer.

Gérez l'accès à Comptes AWS

AWS IAM Identity Center est intégré à AWS Organizations, ce qui vous permet de gérer de manière centralisée les autorisations sur plusieurs comptes Comptes AWS sans configurer manuellement chacun de vos comptes. Vous pouvez définir des autorisations et les attribuer aux utilisateurs du personnel afin de contrôler leur accès à des informations spécifiques Comptes AWS.

Compte AWS types

Il existe deux types d' Comptes AWS entrées AWS Organizations :

- Compte de gestion - Le Compte AWS compte utilisé pour créer l'organisation.
- Comptes de membres : les Comptes AWS autres comptes appartiennent à une organisation.

Pour plus d'informations sur les Compte AWS types, reportez-vous à AWS Organizations la section Terminologie et concepts du guide de AWS Organizations l'utilisateur.

Vous pouvez également choisir d'enregistrer un compte membre en tant qu'administrateur délégué pour IAM Identity Center. Les utilisateurs de ce compte peuvent effectuer la plupart des tâches administratives d'IAM Identity Center. Pour plus d'informations, consultez Administration déléguée.

Pour chaque tâche et chaque type de compte, le tableau suivant indique si la tâche administrative d'IAM Identity Center peut être exécutée par les utilisateurs du compte.

Tâches administratives d'IAM Identity Center	Compte membre	Compte administrateur délégué	Compte de gestion
Lire les utilisateurs ou les groupes (lire le groupe lui-même et les membres du groupe)	 Oui	 Oui	 Oui

Tâches administratives d'IAM Identity Center	Compte membre	Compte administrateur délégué	Compte de gestion
Ajouter, modifier ou supprimer des utilisateurs ou des groupes	Non	Oui	Oui
Activer ou désactiver l'accès utilisateur	Non	Oui	Oui
Activer, désactiver ou gérer les attributs entrants	Non	Oui	Oui
Modifier ou gérer les sources d'identité	Non	Oui	Oui
Création, modification ou suppression d'applications	Non	Oui	Oui
Configuration de la MFA	Non	Oui	Oui

Tâches administratives d'IAM Identity Center	Compte membre	Compte administrateur délégué	Compte de gestion
Gérer les ensembles d'autorisations non provisionnés dans le compte de gestion	Non	Oui	Oui
Gérer les ensembles d'autorisations fournis dans le compte de gestion	Non	Non	Oui
Activer IAM Identity Center	Non	Non	Oui
Supprimer la configuration du centre d'identité IAM	Non	Non	Oui
Activer ou désactiver l'accès utilisateur dans le compte de gestion	Non	Non	Oui
Enregistrer ou désenregistrer un compte membre en tant qu'administrateur délégué	Non	Non	Oui

Attribution d'un accès Compte AWS

Vous pouvez utiliser des ensembles d'autorisations pour simplifier la façon dont vous attribuez l'accès aux utilisateurs et aux groupes de votre organisation Comptes AWS. Les ensembles d'autorisations sont stockés dans IAM Identity Center et définissent le niveau d'accès des utilisateurs et des groupes à un Compte AWS. Vous pouvez créer un ensemble d'autorisations unique et l'attribuer à plusieurs Comptes AWS au sein de votre organisation. Vous pouvez également attribuer plusieurs ensembles d'autorisations au même utilisateur.

Pour plus d'informations sur les jeux d'autorisations, consultez Création, gestion et suppression d'ensembles d'autorisations.

> **Note**
>
> Vous pouvez également attribuer à vos utilisateurs un accès par authentification unique aux applications. Pour plus d'informations, veuillez consulter Gérez l'accès aux applications.

Expérience de l'utilisateur final

Le portail AWS d'accès fournit aux utilisateurs d'IAM Identity Center un accès par authentification unique à toutes les applications Comptes AWS et applications qui leur sont assignées via un portail Web. Le portail AWS d'accès est différent du AWS Management Console, qui est un ensemble de consoles de service permettant de gérer les AWS ressources.

Lorsque vous créez un ensemble d'autorisations, le nom que vous spécifiez pour l'ensemble d'autorisations apparaît dans le portail AWS d'accès en tant que rôle disponible. Les utilisateurs se connectent AWS au portail d'accès Compte AWS, choisissent un, puis le rôle. Une fois qu'ils ont choisi le rôle, ils peuvent accéder aux AWS services en utilisant les informations d'identification temporaires AWS Management Console ou en récupérant des informations d'identification temporaires pour accéder aux AWS services par programmation.

Pour ouvrir AWS Management Console ou récupérer des informations d'identification temporaires afin d'y accéder AWS par programmation, les utilisateurs effectuent les étapes suivantes :

1. Les utilisateurs ouvrent une fenêtre de navigateur et utilisent l'URL de connexion que vous fournissez pour accéder au portail AWS d'accès.
2. À l'aide de leurs identifiants d'annuaire, ils se connectent au portail AWS d'accès.

3. Après authentification, sur la page du portail d' AWS accès, ils choisissent l'onglet Comptes pour afficher la liste des comptes Comptes AWS auxquels ils ont accès.
4. Les utilisateurs choisissent ensuite Compte AWS celui qu'ils souhaitent utiliser.
5. Sous le nom du Compte AWS, tous les ensembles d'autorisations auxquels les utilisateurs sont affectés apparaissent sous forme de rôles disponibles. Par exemple, si vous avez attribué un utilisateur `john_stiles` à l'ensemble d'`PowerUser`autorisations, le rôle s'affiche dans le portail AWS d'accès sous la forme`PowerUser/john_stiles`. Les utilisateurs qui bénéficient de plusieurs jeux d'autorisations choisissent le rôle à utiliser. Les utilisateurs peuvent choisir leur rôle pour accéder au AWS Management Console.
6. Outre le rôle, les utilisateurs du portail AWS d'accès peuvent récupérer des informations d'identification temporaires pour l'accès par ligne de commande ou par programmation en choisissant les clés d'accès.

Pour step-by-step obtenir des conseils que vous pouvez fournir aux utilisateurs de votre personnel, consultez Utilisation du portail AWS d'accès etObtention des informations d'identification utilisateur d'IAM Identity Center pour les SDK AWS CLI ou AWS.

Faire respecter et limiter l'accès

Lorsque vous activez IAM Identity Center, IAM Identity Center crée un rôle lié à un service. Vous pouvez également utiliser des politiques de contrôle des services (SCP).

Délégation et renforcement de l'accès

Un rôle lié à un service est un type de rôle IAM directement lié à un service. AWS Une fois que vous avez activé IAM Identity Center, IAM Identity Center peut créer un rôle lié à un service dans chacun Compte AWS des membres de votre organisation. Ce rôle fournit des autorisations prédéfinies qui permettent à IAM Identity Center de déléguer et d'appliquer les utilisateurs disposant d'un accès par authentification unique à des utilisateurs spécifiques de votre organisation Comptes AWS dans. AWS Organizations Pour utiliser ce rôle, vous devez attribuer à un ou plusieurs utilisateurs l'accès à un compte. Pour plus d'informations, consultez Rôles liés à un service et Utilisation de rôles liés à un service pour IAM Identity Center.

Limiter l'accès à la banque d'identités depuis les comptes des membres

Pour le service de banque d'identité utilisé par IAM Identity Center, les utilisateurs ayant accès à un compte membre peuvent utiliser des actions d'API qui nécessitent des autorisations de lecture.

Les comptes membres ont accès aux actions Read sur les espaces de noms sso-directory et identitystore. Pour plus d'informations, consultez les sections Actions, ressources et clés de condition pour le AWS IAM Identity Center répertoire et Actions, ressources et clés de condition pour AWS Identity Store dans la référence d'autorisation de service.

Pour empêcher les utilisateurs des comptes membres d'utiliser les opérations d'API dans le magasin d'identités, vous pouvez joindre une politique de contrôle des services (SCP). Un SCP est un type de politique d'organisation que vous pouvez utiliser pour gérer les autorisations au sein de votre organisation. L'exemple de SCP suivant empêche les utilisateurs des comptes membres d'accéder à toute opération d'API dans le magasin d'identités.

```
{
    "Sid": "ExplicitlyBlockIdentityStoreAccess",
    "Effect": "Deny",
    "Action": "identitystore:*", "sso-directory:*"],
    "Resource": "*"
}
```

> **Note**
>
> La limitation de l'accès aux comptes des membres peut affecter les fonctionnalités des applications compatibles avec IAM Identity Center.

Pour plus d'informations, consultez Politiques de contrôle de service (SCP) dans le Guide de l'utilisateur AWS Organizations .

Administration déléguée

L'administration déléguée permet aux utilisateurs assignés à un compte membre enregistré d'effectuer facilement la plupart des tâches administratives d'IAM Identity Center. Lorsque vous activez IAM Identity Center, votre instance IAM Identity Center est créée AWS Organizations par défaut dans le compte de gestion. Cela a été initialement conçu de cette façon afin qu'IAM Identity Center puisse fournir, déprovisionner et mettre à jour les rôles sur tous les comptes membres de votre organisation. Même si votre instance IAM Identity Center doit toujours résider dans le compte de gestion, vous pouvez choisir de déléguer l'administration d'IAM Identity Center à un compte membre AWS Organizations, étendant ainsi la capacité de gérer IAM Identity Center depuis l'extérieur du compte de gestion.

L'activation de l'administration déléguée offre les avantages suivants :

- Minimise le nombre de personnes ayant besoin d'accéder au compte de gestion pour atténuer les problèmes de sécurité
- Permet à certains administrateurs d'attribuer des utilisateurs et des groupes aux applications et aux comptes des membres de votre organisation

Pour plus d'informations sur le fonctionnement d'IAM Identity Center AWS Organizations, consultezGérez l'accès à Comptes AWS. Pour plus d'informations et pour consulter un exemple de scénario d'entreprise montrant comment configurer l'administration déléguée, consultez Getting started with IAM Identity Center Delegated Administration dans le blog AWS de sécurité.

Rubriques

Bonnes pratiques

Voici quelques bonnes pratiques à prendre en compte avant de configurer l'administration déléguée.

- Accorder le moindre privilège au compte de gestion — Sachant que le compte de gestion est un compte hautement privilégié et pour respecter le principe du moindre privilège, nous vous recommandons vivement de restreindre l'accès au compte de gestion au moins de personnes possible. La fonctionnalité d'administrateur délégué vise à minimiser le nombre de personnes ayant besoin d'accéder au compte de gestion.
- Créez des ensembles d'autorisations à utiliser uniquement dans le compte de gestion : cela facilite l'administration des ensembles d'autorisations adaptés uniquement aux utilisateurs accédant à votre compte de gestion et permet de les différencier des ensembles d'autorisations gérés par votre compte d'administrateur délégué.
- Tenez compte de votre emplacement Active Directory : si vous prévoyez d'utiliser Active Directory comme source d'identité IAM Identity Center, localisez le répertoire dans le compte membre sur lequel vous avez activé la fonctionnalité d'administrateur délégué d'IAM Identity Center. Si

vous décidez de remplacer la source d'identité IAM Identity Center d'une autre source par Active Directory, ou de la remplacer par une autre source, le répertoire doit résider dans le compte membre administrateur délégué d'IAM Identity Center (s'il en existe un) ; sinon, il doit se trouver dans le compte de gestion.

- Créer des attributions d'utilisateurs uniquement dans le compte de gestion : l'administrateur délégué ne peut pas modifier les ensembles d'autorisations fournis dans le compte de gestion. Toutefois, les administrateurs délégués peuvent ajouter, modifier et supprimer des groupes et des attributions de groupes.

Prérequis

Avant de pouvoir enregistrer un compte en tant qu'administrateur délégué, vous devez d'abord déployer l'environnement suivant :

- AWS Organizations doit être activé et configuré avec au moins un compte membre en plus de votre compte de gestion par défaut.
- Si votre source d'identité est définie sur Active Directory, la Synchronisation AD configurable par IAM Identity Center fonctionnalité doit être activée.

Enregistrez un compte membre

Pour configurer l'administration déléguée, vous devez d'abord enregistrer un compte de membre dans votre organisation en tant qu'administrateur délégué. Les utilisateurs de ce compte membre disposant d'autorisations suffisantes auront un accès administratif à IAM Identity Center. Une fois qu'un compte membre est enregistré avec succès pour l'administration déléguée, il est appelé compte d'administrateur délégué. Pour en savoir plus sur les tâches que le compte administrateur délégué peut effectuer, consultezCompte AWS types.

IAM Identity Center prend en charge l'enregistrement d'un seul compte membre en tant qu'administrateur délégué à la fois. Vous ne pouvez créer un compte membre que lorsque vous êtes connecté avec les informations d'identification du compte de gestion.

Utilisez la procédure suivante pour accorder un accès administratif à IAM Identity Center en enregistrant un compte de membre spécifique dans votre AWS organisation en tant qu'administrateur délégué.

Important

Cette opération délègue l'accès administratif d'IAM Identity Center aux utilisateurs administrateurs de ce compte membre. Tous les utilisateurs disposant d'autorisations suffisantes pour ce compte d'administrateur délégué peuvent effectuer toutes les tâches administratives d'IAM Identity Center à partir de ce compte, à l'exception de :

- Activation du centre d'identité IAM
- Suppression des configurations du centre d'identité IAM
- Gestion des ensembles d'autorisations fournis dans le compte de gestion
- Enregistrer ou désenregistrer d'autres comptes membres en tant qu'administrateurs délégués
- Activation ou désactivation de l'accès utilisateur dans le compte de gestion

L'administrateur délégué peut modifier l'appartenance au groupe.

Pour créer un compte membre

1. Connectez-vous à l' AWS Management Console aide des informations d'identification de votre compte de gestion dans AWS Organizations. Les informations d'identification du compte de gestion sont requises pour exécuter l'RegisterDelegatedAdministratorAPI.
2. Sélectionnez la région dans laquelle IAM Identity Center est activé, puis ouvrez la console IAM Identity Center.
3. Choisissez Paramètres, puis sélectionnez l'onglet Gestion.
4. Dans la section Administrateur délégué, choisissez Enregistrer un compte.
5. Sur la page Enregistrer un administrateur délégué, sélectionnez celui que Compte AWS vous souhaitez enregistrer, puis choisissez Enregistrer un compte.

Annuler l'enregistrement d'un compte membre

Vous ne pouvez annuler l'enregistrement d'un compte membre que lorsque vous êtes connecté avec les informations d'identification du compte de gestion.

Utilisez la procédure suivante pour supprimer l'accès administratif à IAM Identity Center en annulant l'enregistrement d'un compte de membre de votre AWS organisation qui avait été précédemment désigné comme administrateur délégué.

> **Important**
>
> Lorsque vous désenregistrez un compte, vous empêchez effectivement tous les utilisateurs administrateurs de gérer IAM Identity Center à partir de ce compte. Par conséquent, ils ne peuvent plus administrer les identités IAM Identity Center, la gestion des accès, l'authentification ou l'accès aux applications à partir de ce compte. Cette opération n'affectera aucune autorisation ou attribution configurée dans IAM Identity Center et n'aura donc aucun impact sur vos utilisateurs finaux, car ils continueront d'avoir accès à leurs applications et Comptes AWS depuis le portail AWS d'accès.

Pour annuler l'enregistrement d'un compte de membre

1. Connectez-vous à l' AWS Management Console aide des informations d'identification de votre compte de gestion dans AWS Organizations. Les informations d'identification du compte de gestion sont requises pour exécuter l'DeregisterDelegatedAdministratorAPI.
2. Sélectionnez la région dans laquelle IAM Identity Center est activé, puis ouvrez la console IAM Identity Center.
3. Choisissez Paramètres, puis sélectionnez l'onglet Gestion.
4. Dans la section Administrateur délégué, choisissez Désenregistrer le compte.
5. Dans la boîte de dialogue Désenregistrer le compte, examinez les implications en matière de sécurité, puis entrez le nom du compte membre pour confirmer que vous avez bien compris.
6. Choisissez Désenregistrer le compte.

Afficher quel compte de membre a été enregistré en tant qu'administrateur délégué

Suivez la procédure ci-dessous pour savoir quel compte de membre AWS Organizations a été configuré en tant qu'administrateur délégué pour IAM Identity Center.

Pour consulter votre compte de membre enregistré

1. Ouvrez la console IAM Identity Center.

2. Sélectionnez Settings (Paramètres).
3. Dans la section Détails, recherchez le nom du compte enregistré sous Administrateur délégué. Vous pouvez également trouver ces informations en sélectionnant l'onglet Gestion et en les consultant dans la section Administrateur délégué.

Accès surélevé temporaire

Tout accès à votre compte Compte AWS implique un certain niveau de privilège. Les opérations sensibles, telles que la modification de la configuration d'une ressource de grande valeur, par exemple un environnement de production, nécessitent un traitement spécial en raison de leur portée et de leur impact potentiel. L'accès élevé temporaire (également appelé just-in-time accès) est un moyen de demander, d'approuver et de suivre l'utilisation d'une autorisation pour effectuer une tâche spécifique pendant une période spécifiée. L'accès élevé temporaire complète d'autres formes de contrôle d'accès, telles que les ensembles d'autorisations et l'authentification multifactorielle.

AWS IAM Identity Center propose les options suivantes pour la gestion temporaire des accès élevés dans différents environnements commerciaux et techniques :

- Solutions gérées et prises en charge par le fournisseur : AWS a validé les intégrations IAM Identity Center des offres de certains partenaires et évalué leurs capacités par rapport à un ensemble commun d'exigences clients. Choisissez la solution qui correspond le mieux à votre scénario et suivez les instructions du fournisseur pour activer cette fonctionnalité avec IAM Identity Center.
- Autogéré et autonome : cette option constitue un point de départ si vous êtes intéressé par un accès élevé temporaire AWS uniquement et que vous pouvez déployer, adapter et gérer vous-même cette fonctionnalité. Pour plus d'informations, consultez la section Gestion des accès élevés temporaires (TEAM).

Partenaires AWS de sécurité validés pour un accès élevé temporaire

AWS Les partenaires de sécurité utilisent différentes approches pour répondre à un ensemble commun d'exigences d'accès temporaire élevé. Nous vous recommandons d'examiner attentivement chaque solution partenaire afin de choisir celle qui correspond le mieux à vos besoins et préférences, notamment à votre activité, à l'architecture de votre environnement cloud et à votre budget.

> **Note**
>
> Pour la reprise après sinistre, nous vous recommandons de configurer un accès d'urgence au AWS Management Console avant qu'une interruption ne survienne.

AWS Identity a validé les fonctionnalités et l'intégration avec IAM Identity Center pour les just-in-time offres suivantes des partenaires de AWS sécurité :

- CyberArk Secure Cloud Access— Cette offre fournit notamment un accès élevé à la demande à des environnements multicloud AWS et à des environnements multicloud. CyberArk Identity Security Platform Les approbations sont traitées par le biais de l'intégration à l'ITSM ou à l' ChatOps outillage. Toutes les sessions peuvent être enregistrées à des fins d'audit et de conformité.
- Tenable (previously Ermetic)— La Tenable plate-forme inclut la fourniture d'un accès just-in-time privilégié pour les opérations administratives dans les environnements multicloud AWS et multicloud. Les journaux de session de tous les environnements cloud, y compris les journaux AWS CloudTrail d'accès, sont disponibles dans une interface unique à des fins d'analyse et d'audit. Cette fonctionnalité s'intègre aux outils d'entreprise et de développement tels que Slack et Microsoft Teams.
- OktaDemandes d'accès : partie intégrante de la gouvernance des Okta identités, vous permet de configurer un flux de travail de demandes d' just-in-time accès en utilisant en Okta tant que fournisseur d'identité externe (IdP) IAM Identity Center et vos ensembles d'autorisations IAM Identity Center.

Cette liste sera mise à jour afin de AWS valider les capacités des solutions partenaires supplémentaires et l'intégration de ces solutions à IAM Identity Center.

> **Note**
>
> Si vous utilisez des politiques basées sur les ressources, consultez Amazon Elastic Kubernetes Service (Amazon EKS AWS Key Management Service) ou (Référencement des ensembles d'autorisations dans les politiques de ressources, Amazon EKS et AWS KMS) avant AWS KMS de choisir votre solution. just-in-time

Capacités d'accès élevé temporaires évaluées en vue de la validation par les AWS partenaires

AWS Identity a confirmé que les fonctionnalités d'accès élevé temporaires proposées par CyberArk Secure Cloud AccessTenable, et les demandes Okta d'accès répondent aux exigences courantes suivantes des clients :

- Les utilisateurs peuvent demander l'accès à un ensemble d'autorisations pour une période spécifiée par l'utilisateur, en spécifiant le AWS compte, l'ensemble d'autorisations, la période et le motif.
- Les utilisateurs peuvent recevoir le statut d'approbation de leur demande.
- Les utilisateurs ne peuvent pas appeler une session ayant une portée donnée, sauf s'il existe une demande approuvée ayant la même portée et s'ils appellent la session pendant la période approuvée.
- Il existe un moyen de spécifier qui peut approuver les demandes.
- Les approbateurs ne peuvent pas approuver leurs propres demandes.
- Les approbateurs disposent d'une liste des demandes en attente, approuvées et rejetées et peuvent l'exporter pour les auditeurs.
- Les approbateurs peuvent approuver et rejeter les demandes en attente.
- Les approbateurs peuvent ajouter une note expliquant leur décision.
- Les approbateurs peuvent révoquer une demande approuvée, empêchant ainsi l'utilisation future d'un accès élevé.

> **Note**
>
> Si un utilisateur est connecté avec un accès élevé lorsqu'une demande approuvée est révoquée, sa session reste active jusqu'à une heure après la révocation de l'approbation. Pour plus d'informations sur les sessions d'authentification, consultezAuthentification.

- Les actions et approbations des utilisateurs sont disponibles pour audit.

Accès par authentification unique à Comptes AWS

Vous pouvez attribuer aux utilisateurs de votre annuaire connecté des autorisations d'accès au compte de gestion ou aux comptes de membres de votre organisation en AWS Organizations

fonction des fonctions professionnelles courantes. Vous pouvez également utiliser des autorisations personnalisées pour répondre à vos spécifications de sécurité spécifiques. Par exemple, vous pouvez accorder aux administrateurs de base de données des autorisations étendues sur Amazon RDS dans les comptes de développement, mais limiter leurs autorisations dans les comptes de production. IAM Identity Center configure automatiquement toutes les autorisations utilisateur nécessaires dans votre Comptes AWS système.

> **Note**
>
> Vous devrez peut-être accorder à des utilisateurs ou à des groupes des autorisations pour opérer dans le compte AWS Organizations de gestion. Comme il s'agit d'un compte à privilèges élevés, des restrictions de sécurité supplémentaires nécessitent que vous disposiez de la FullAccess politique IAM ou d'autorisations équivalentes avant de pouvoir le configurer. Ces restrictions de sécurité supplémentaires ne sont requises pour aucun des comptes membres de votre AWS organisation.

Attribuer un accès utilisateur à Comptes AWS

Utilisez la procédure suivante pour attribuer un accès par authentification unique aux utilisateurs et aux groupes de votre annuaire connecté et utiliser des ensembles d'autorisations pour déterminer leur niveau d'accès.

Pour vérifier l'accès des utilisateurs et des groupes existants, voirAfficher les attributions des utilisateurs et des groupes.

> **Note**
>
> Pour simplifier l'administration des autorisations d'accès, nous vous recommandons d'attribuer l'accès directement aux groupes et non pas aux différents utilisateurs. Avec les groupes, vous pouvez accorder ou refuser des autorisations à des groupes d'utilisateurs au lieu d'avoir à les appliquer individuellement à chaque utilisateur. Si un utilisateur change d'organisation, il vous suffit de le déplacer dans un autre groupe et il reçoit automatiquement les autorisations nécessaires pour la nouvelle organisation.

Pour attribuer un accès à un utilisateur ou à un groupe à Comptes AWS

1. Ouvrez la console IAM Identity Center.

> **Note**
>
> Assurez-vous que la console IAM Identity Center utilise la région dans laquelle se trouve votre AWS Managed Microsoft AD répertoire avant de passer à l'étape suivante.

2. Dans le volet de navigation, sous Autorisations multi-comptes, sélectionnez Comptes AWS.
3. Sur la Comptes AWSpage, une liste arborescente de votre organisation apparaît. Cochez la case à côté d'une ou de plusieurs Comptes AWS personnes auxquelles vous souhaitez attribuer un accès par authentification unique.

   > **Note**
   >
   > Vous pouvez en sélectionner jusqu'à 10 Comptes AWS à la fois par ensemble d'autorisations lorsque vous attribuez un accès par authentification unique à des utilisateurs et à des groupes. Pour en attribuer plus de 10 Comptes AWS au même ensemble d'utilisateurs et de groupes, répétez cette procédure selon les besoins pour les comptes supplémentaires. Lorsque vous y êtes invité, sélectionnez les mêmes utilisateurs, groupes et ensembles d'autorisations.

4. Choisissez Attribuer des utilisateurs ou des groupes.
5. Pour l'étape 1 : Sélectionnez les utilisateurs et les groupes, sur la page Affecter des utilisateurs et des groupes à « ***AWS-account-name*** », procédez comme suit :

   1. Dans l'onglet Utilisateurs, sélectionnez un ou plusieurs utilisateurs auxquels vous souhaitez accorder l'accès par authentification unique.

      Pour filtrer les résultats, commencez à saisir le nom de l'utilisateur souhaité dans le champ de recherche.

   2. Dans l'onglet Groupes, sélectionnez un ou plusieurs groupes auxquels vous souhaitez accorder un accès par authentification unique.

      Pour filtrer les résultats, commencez à taper le nom du groupe souhaité dans le champ de recherche.

   3. Pour afficher les utilisateurs et les groupes que vous avez sélectionnés, choisissez le triangle latéral à côté de Utilisateurs et groupes sélectionnés.

4. Après avoir confirmé que les utilisateurs et les groupes sélectionnés sont corrects, choisissez Next.

6. Pour l'étape 2 : sélectionner des ensembles d'autorisations, sur la page Attribuer des ensembles d'autorisations à « ***AWS-account-name*** », procédez comme suit :

   1. Sélectionnez un ou plusieurs ensembles d'autorisations. Si nécessaire, vous pouvez créer et sélectionner de nouveaux ensembles d'autorisations.

      - Pour sélectionner un ou plusieurs ensembles d'autorisations existants, sous Ensembles d'autorisations, sélectionnez les ensembles d'autorisations que vous souhaitez appliquer aux utilisateurs et aux groupes que vous avez sélectionnés à l'étape précédente.
      - Pour créer un ou plusieurs nouveaux ensembles d'autorisations, choisissez Créer un ensemble d'autorisations et suivez les étapes décrites dansCrée un jeu d'autorisations.. Après avoir créé les ensembles d'autorisations que vous souhaitez appliquer, dans la console IAM Identity Center, revenez Comptes AWSet suivez les instructions jusqu'à ce que vous atteigniez l'étape 2 : Sélectionnez les ensembles d'autorisations. Lorsque vous atteignez cette étape, sélectionnez les nouveaux ensembles d'autorisations que vous avez créés et passez à l'étape suivante de cette procédure.

   2. Après avoir confirmé que les ensembles d'autorisations appropriés sont sélectionnés, choisissez Next.

7. Pour l'étape 3 : Révision et envoi, sur la page Réviser et envoyer les assignations à « ***AWS-account-name*** », procédez comme suit :

   1. Passez en revue les utilisateurs, les groupes et les ensembles d'autorisations sélectionnés.
   2. Après avoir confirmé que les utilisateurs, groupes et ensembles d'autorisations appropriés sont sélectionnés, choisissez Soumettre.

      > **Important**
      >
      > Le processus d'attribution des utilisateurs et des groupes peut prendre quelques minutes. Laissez cette page ouverte jusqu'à ce que le processus soit terminé avec succès.

> **Note**
>
> Vous devrez peut-être accorder à des utilisateurs ou à des groupes des autorisations pour opérer dans le compte AWS Organizations de gestion. Comme il s'agit d'un compte à privilèges élevés, des restrictions de sécurité supplémentaires nécessitent que vous disposiez de la FullAccess politique IAM ou d'autorisations équivalentes avant de pouvoir le configurer. Ces restrictions de sécurité supplémentaires ne sont requises pour aucun des comptes membres de votre AWS organisation.

Supprimer l'accès des utilisateurs et des groupes

Utilisez cette procédure pour supprimer l'accès par authentification unique Compte AWS à un ou plusieurs utilisateurs et groupes de votre annuaire connecté.

Pour supprimer l'accès des utilisateurs et des groupes à un Compte AWS

1. Ouvrez la console IAM Identity Center.
2. Dans le volet de navigation, sous Autorisations multi-comptes, sélectionnez Comptes AWS.
3. Sur la Comptes AWSpage, une liste arborescente de votre organisation apparaît. Sélectionnez le nom Compte AWS qui contient les utilisateurs et les groupes pour lesquels vous souhaitez supprimer l'accès par authentification unique.
4. Sur la page d'aperçu de Compte AWS, sous Utilisateurs et groupes assignés, sélectionnez le nom d'un ou de plusieurs utilisateurs ou groupes, puis choisissez Supprimer l'accès.
5. Dans la boîte de dialogue Supprimer l'accès, vérifiez que les noms des utilisateurs ou des groupes sont corrects, puis choisissez Supprimer l'accès.

Révoquer les sessions de rôle IAM actives créées par des ensembles d'autorisations

La procédure générale suivante permet de révoquer une session d'ensemble d'autorisations active pour un utilisateur d'IAM Identity Center. La procédure part du principe que vous souhaitez supprimer tout accès à un utilisateur dont les informations d'identification ont été compromises ou à un acteur malveillant présent dans le système. La condition préalable est d'avoir suivi les directives enPréparez-vous à révoquer une session de rôle IAM active créée par un ensemble d'autorisations.

Nous supposons que la politique de refus de tout est présente dans une politique de contrôle des services (SCP).

> **Note**
>
> AWS vous recommande de créer une automatisation pour gérer toutes les étapes, à l'exception des opérations relatives à la console uniquement.

1. Obtenez le nom d'utilisateur de la personne dont vous devez révoquer l'accès. Vous pouvez utiliser les API du magasin d'identités pour trouver l'utilisateur à l'aide de son nom d'utilisateur.
2. Mettez à jour la politique de refus pour ajouter l'ID utilisateur de l'étape 1 dans votre politique de contrôle des services (SCP). Une fois cette étape terminée, l'utilisateur cible perd son accès et n'est plus en mesure d'effectuer des actions avec les rôles concernés par la politique.
3. Supprimez tous les ensembles d'autorisations attribués à l'utilisateur. Si l'accès est attribué par le biais d'appartenances à des groupes, supprimez l'utilisateur de tous les groupes et de toutes les attributions directes d'ensembles d'autorisations. Cette étape empêche l'utilisateur d'assumer des rôles IAM supplémentaires. Si un utilisateur possède une session active sur le portail d' AWS accès et que vous le désactivez, il peut continuer à assumer de nouveaux rôles jusqu'à ce que vous supprimiez son accès.
4. Si vous utilisez un fournisseur d'identité (IdP) ou Microsoft Active Directory comme source d'identité, désactivez l'utilisateur dans la source d'identité. La désactivation de l'utilisateur empêche la création de sessions supplémentaires sur le portail AWS d'accès. Utilisez la documentation de votre IdP ou de l'API Microsoft Active Directory pour savoir comment automatiser cette étape. Si vous utilisez le répertoire IAM Identity Center comme source d'identité, ne désactivez pas encore l'accès des utilisateurs. Vous allez désactiver l'accès des utilisateurs à l'étape 6.
5. Dans la console IAM Identity Center, recherchez l'utilisateur et supprimez sa session active.
   a. Choisissez Utilisateurs.
   b. Choisissez l'utilisateur dont vous souhaitez supprimer la session active.
   c. Sur la page détaillée de l'utilisateur, choisissez l'onglet Sessions actives.
   d. Cochez les cases à côté des sessions que vous souhaitez supprimer et choisissez Supprimer la session.

Cela garantit que la session du portail d' AWS accès de l'utilisateur s'arrête dans un délai d'environ 60 minutes. En savoir plus sur la durée des sessions.

6. Dans la console IAM Identity Center, désactivez l'accès des utilisateurs.

   a. Choisissez Utilisateurs.

   b. Choisissez l'utilisateur dont vous souhaitez désactiver l'accès.

   c. Sur la page détaillée de l'utilisateur, développez Informations générales et cliquez sur le bouton Désactiver l'accès utilisateur pour empêcher toute nouvelle connexion de l'utilisateur.

7. Laissez la politique de refus en place pendant au moins 12 heures. Dans le cas contraire, l'utilisateur disposant d'une session de rôle IAM active aura restauré les actions avec le rôle IAM. Si vous attendez 12 heures, les sessions actives expirent et l'utilisateur ne pourra plus accéder au rôle IAM.

> **Important**
>
> Si vous désactivez l'accès d'un utilisateur avant d'arrêter la session utilisateur (vous avez effectué l'étape 6 sans terminer l'étape 5), vous ne pouvez plus arrêter la session utilisateur via la console IAM Identity Center. Si vous désactivez par inadvertance l'accès utilisateur avant d'arrêter la session utilisateur, vous pouvez réactiver l'utilisateur, arrêter sa session, puis désactiver à nouveau son accès.

Vous pouvez désormais modifier les informations d'identification de l'utilisateur si son mot de passe a été compromis et rétablir ses attributions.

Déléguer les personnes habilitées à attribuer un accès d'authentification unique aux utilisateurs et aux groupes du compte de gestion

L'attribution d'un accès d'authentification unique au compte de gestion à l'aide de la console IAM Identity Center est une action privilégiée. Par défaut, seul un Utilisateur racine d'un compte AWS ou un utilisateur auquel AWSSSOMasterAccountAdministratorles politiques IAMFullAccess AWS gérées sont associées peut attribuer un accès par authentification unique au compte de gestion. Les IAMFullAccesspolitiques AWSSSOMasterAccountAdministratoret gèrent l'accès par authentification unique au compte de gestion au sein d'une AWS Organizations organisation.

Suivez les étapes ci-dessous pour déléguer des autorisations afin de gérer l'accès par authentification unique aux utilisateurs et aux groupes de votre annuaire.

Pour accorder des autorisations permettant de gérer l'accès par authentification unique aux utilisateurs et aux groupes de votre annuaire

1. Connectez-vous à la console IAM Identity Center en tant qu'utilisateur root du compte de gestion ou avec un autre utilisateur disposant d'autorisations d'administrateur sur le compte de gestion.
2. Suivez les étapes décrites Crée un jeu d'autorisations. pour créer un ensemble d'autorisations, puis procédez comme suit :

    1. Sur la page Créer un nouvel ensemble d'autorisations, cochez la case Créer un ensemble d'autorisations personnalisé, puis choisissez Suivant : Détails.
    2. Sur la page Créer un nouvel ensemble d'autorisations, spécifiez un nom pour le jeu d'autorisations personnalisé et, éventuellement, une description. Si nécessaire, modifiez la durée de la session et spécifiez l'URL de l'état du relais.

        > **Note**
        >
        > Pour l'URL de l'état du relais, vous devez spécifier une URL qui se trouve dans le AWS Management Console. Par exemple : **`https://console.aws.amazon.com/ec2/`**
        > Pour plus d'informations, consultez Définir l'état du relais.

    3. Sous Quelles politiques souhaitez-vous inclure dans votre ensemble d'autorisations ? , cochez la case Joindre les politiques AWS gérées.
    4. Dans la liste des politiques IAM, sélectionnez à la fois les politiques AWSSSOMasterAccountAdministratoret les politiques IAMFullAccess AWS gérées. Ces politiques accordent des autorisations à tous les utilisateurs et groupes auxquels l'accès à cet ensemble d'autorisations sera attribué à l'avenir.
    5. Choisissez Suivant : Balises.
    6. Sous Ajouter des balises (facultatif), spécifiez les valeurs de clé et de valeur (facultatif), puis choisissez Suivant : Révision. Pour en savoir plus sur les identifications, consultez Balisage de ressources AWS IAM Identity Center.
    7. Passez en revue les sélections que vous avez effectuées, puis choisissez Créer.
3. Suivez les étapes décrites Attribuer un accès utilisateur à Comptes AWS pour attribuer les utilisateurs et les groupes appropriés à l'ensemble d'autorisations que vous venez de créer.

4. Communiquez ce qui suit aux utilisateurs assignés : lorsqu'ils se connectent au portail AWS d'accès et choisissent l'onglet Comptes, ils doivent choisir le nom de rôle approprié pour être authentifiés avec les autorisations que vous venez de déléguer.

Jeux d'autorisations

Un ensemble d'autorisations est un modèle que vous créez et gérez qui définit un ensemble d'une ou plusieurs politiques IAM. Les ensembles d'autorisations simplifient l'attribution des Compte AWS accès aux utilisateurs et aux groupes de votre organisation. Par exemple, vous pouvez créer un ensemble d'autorisations d'administrateur de base de données qui inclut des politiques d'administration des services AWS RDS, DynamoDB et Aurora, et utiliser cet ensemble d'autorisations unique pour accorder l'accès à une liste de cibles AWS au sein de votre organisation à vos administrateurs Comptes AWS de base de données.

IAM Identity Center attribue l'accès à un utilisateur ou à un groupe dans un ou plusieurs ensembles Comptes AWS d'autorisations. Lorsque vous attribuez un ensemble d'autorisations, IAM Identity Center crée les rôles IAM contrôlés par IAM Identity Center correspondants dans chaque compte et associe les politiques spécifiées dans le jeu d'autorisations à ces rôles. IAM Identity Center gère le rôle et permet aux utilisateurs autorisés que vous avez définis d'assumer ce rôle à l'aide du portail utilisateur ou de la CLI AWS d'IAM Identity Center. Lorsque vous modifiez l'ensemble d'autorisations, IAM Identity Center veille à ce que les politiques et rôles IAM correspondants soient mis à jour en conséquence.

Vous pouvez ajouter des politiques AWS gérées, des politiques gérées par le client, des politiques intégrées et des politiques AWS gérées pour les fonctions professionnelles à vos ensembles d'autorisations. Vous pouvez également attribuer une politique AWS gérée ou une politique gérée par le client comme limite d'autorisation.

Pour créer un ensemble d'autorisations, voirCréation, gestion et suppression d'ensembles d'autorisations.

Rubriques

- Autorisations prédéfinies
- Autorisations personnalisées
- Création, gestion et suppression d'ensembles d'autorisations
- Configurer les propriétés des ensembles d'autorisations

Autorisations prédéfinies

Vous pouvez créer un ensemble d'autorisations prédéfini avec des politiques AWS gérées.

Lorsque vous créez un ensemble d'autorisations avec des autorisations prédéfinies, vous choisissez une politique dans une liste de politiques AWS gérées. Parmi les politiques disponibles, vous pouvez choisir entre les politiques d'autorisation communes et les politiques relatives aux fonctions Job.

Politiques d'autorisation communes

Choisissez parmi une liste de politiques AWS gérées qui vous permettent d'accéder aux ressources dans votre intégralité Compte AWS. Vous pouvez ajouter l'une des politiques suivantes :

- AdministratorAccess
- PowerUserAccess
- ReadOnlyAccess
- ViewOnlyAccess

Politiques relatives aux fonctions du poste

Choisissez parmi une liste de politiques AWS gérées qui permettent d'accéder aux ressources de votre organisation Compte AWS susceptibles d'être pertinentes pour un poste au sein de votre organisation. Vous pouvez ajouter l'une des politiques suivantes :

- Billing
- DataScientist
- DatabaseAdministrator
- NetworkAdministrator
- SecurityAudit
- SupportUser
- SystemAdministrator

Pour une description détaillée des politiques d'autorisation communes et des politiques relatives aux fonctions professionnelles disponibles, voir les politiques AWS gérées pour les fonctions professionnelles dans le guide de AWS Identity and Access Management l'utilisateur.

Pour obtenir des instructions sur la création d'un ensemble d'autorisations, consultezCréation, gestion et suppression d'ensembles d'autorisations.

Autorisations personnalisées

Vous pouvez créer un ensemble d'autorisations avec des autorisations personnalisées, en combinant toutes les politiques AWS gérées et gérées par le client que vous avez dans AWS Identity and Access Management (IAM) avec des politiques intégrées. Vous pouvez également inclure une limite d'autorisations, en définissant le maximum d'autorisations que les autres politiques peuvent accorder aux utilisateurs de votre ensemble d'autorisations.

Pour obtenir des instructions sur la création d'un ensemble d'autorisations, consultezCréation, gestion et suppression d'ensembles d'autorisations.

Types de politiques que vous pouvez associer à votre ensemble d'autorisations

Rubriques

- Politiques en ligne
- AWS politiques gérées
- Politiques gérées par le client
- Limites d'autorisations

Politiques en ligne

Vous pouvez associer une politique intégrée à un ensemble d'autorisations. Une politique intégrée est un bloc de texte formaté comme une politique IAM que vous ajoutez directement à votre ensemble d'autorisations. Vous pouvez coller une politique ou en générer une nouvelle à l'aide de l'outil de création de politiques de la console IAM Identity Center lorsque vous créez un nouvel ensemble d'autorisations. Vous pouvez également créer des politiques IAM à l'aide du générateur AWS de politiques.

Lorsque vous déployez un ensemble d'autorisations avec une politique intégrée, IAM Identity Center crée une stratégie IAM à l' Comptes AWS endroit où vous attribuez votre ensemble d'autorisations. IAM Identity Center crée la politique lorsque vous attribuez l'ensemble d'autorisations au compte. La politique est ensuite attachée au rôle IAM Compte AWS que votre utilisateur assume dans votre entreprise.

Lorsque vous créez une politique intégrée et que vous attribuez votre ensemble d'autorisations, IAM Identity Center configure les politiques qui s'y trouvent pour vous Comptes AWS . Lorsque vous créez votre ensemble d'autorisations avecPolitiques gérées par le client, vous devez créer Comptes AWS vous-même les politiques avant d'attribuer l'ensemble d'autorisations.

AWS politiques gérées

Vous pouvez associer des politiques AWS gérées à votre ensemble d'autorisations. AWS les politiques gérées sont des politiques IAM qui AWS maintiennent. En revanche, Politiques gérées par le client les politiques IAM de votre compte sont-elles créées et mises à jour ? AWS les politiques gérées répondent aux cas courants d'utilisation du moindre privilège dans votre Compte AWS Vous pouvez attribuer une politique AWS gérée en tant qu'autorisations pour le rôle créé par IAM Identity Center ou en tant que limite d'autorisations.

AWS maintient des politiques AWS gérées pour les fonctions professionnelles qui attribuent des autorisations d'accès spécifiques à la tâche à vos AWS ressources. Vous pouvez ajouter une politique de fonction professionnelle lorsque vous choisissez d'utiliser des autorisations prédéfinies avec votre ensemble d'autorisations. Lorsque vous choisissez Autorisations personnalisées, vous pouvez ajouter plusieurs règles relatives aux fonctions professionnelles.

Vous contient Compte AWS également un grand nombre de politiques IAM AWS gérées pour des raisons spécifiques Services AWS et combinées de Services AWS. Lorsque vous créez un ensemble d'autorisations avec des autorisations personnalisées, vous pouvez choisir parmi de nombreuses politiques AWS gérées supplémentaires à attribuer à votre ensemble d'autorisations.

AWS remplit chacun d'entre eux Compte AWS avec des politiques AWS gérées. Pour déployer un ensemble d'autorisations avec des politiques AWS gérées, il n'est pas nécessaire de créer au préalable une politique dans votre Comptes AWS. Lorsque vous créez votre ensemble d'autorisations avecPolitiques gérées par le client, vous devez créer Comptes AWS vous-même les politiques avant d'attribuer l'ensemble d'autorisations.

Pour plus d'informations sur les politiques AWS gérées, voir les politiques AWS gérées dans le guide de l'utilisateur IAM.

Politiques gérées par le client

Vous pouvez associer des politiques gérées par le client à votre ensemble d'autorisations. Les politiques gérées par le client sont des politiques IAM de votre compte que vous créez et gérez. En revanche, AWS politiques gérées les politiques IAM de votre compte sont-elles AWS maintenues ? Vous pouvez attribuer une politique gérée par le client en tant qu'autorisations pour le rôle créé par IAM Identity Center ou en tant que limite d'autorisations.

Lorsque vous créez un ensemble d'autorisations avec une politique gérée par le client, vous devez créer une stratégie IAM portant le même nom et le même chemin dans chaque Compte AWS

cas où IAM Identity Center attribue votre ensemble d'autorisations. Si vous spécifiez un chemin personnalisé, assurez-vous de spécifier le même chemin dans chacun d'eux Compte AWS. Pour plus d'informations, consultez Noms conviviaux et chemins dans le Guide de l'utilisateur IAM. IAM Identity Center attache la politique IAM au rôle IAM qu'il crée dans votre. Compte AWS Il est recommandé d'appliquer les mêmes autorisations à la politique dans chaque compte auquel vous attribuez l'ensemble d'autorisations. Pour plus d'informations, consultez Utiliser les politiques IAM dans les ensembles d'autorisations.

Pour plus d'informations, consultez la section Politiques gérées par le client dans le guide de l'utilisateur IAM.

Limites d'autorisations

Vous pouvez associer une limite d'autorisations à votre ensemble d'autorisations. Une limite d'autorisations est une politique IAM AWS gérée ou gérée par le client qui définit le maximum d'autorisations qu'une politique basée sur l'identité peut accorder à un principal IAM. Lorsque vous appliquez une limite d'autorisations Politiques en lignePolitiques gérées par le client, vous ne AWS politiques gérées pouvez pas accorder d'autorisations dépassant les autorisations accordées par votre limite d'autorisations. Une limite d'autorisations n'accorde aucune autorisation, mais fait en sorte qu'IAM ignore toutes les autorisations au-delà de cette limite.

Lorsque vous créez un ensemble d'autorisations avec une politique gérée par le client comme limite d'autorisations, vous devez créer une politique IAM portant le même nom dans chaque Compte AWS cas où IAM Identity Center attribue votre ensemble d'autorisations. IAM Identity Center associe la politique IAM en tant que limite d'autorisation au rôle IAM qu'il crée dans votre. Compte AWS

Pour plus d'informations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.

Création, gestion et suppression d'ensembles d'autorisations

Les ensembles d'autorisations définissent le niveau d'accès des utilisateurs et des groupes à un Compte AWS. Les ensembles d'autorisations sont stockés dans IAM Identity Center et peuvent être fournis à une ou plusieurs personnes. Comptes AWS Vous pouvez attribuer plus d'un jeu d'autorisations à un utilisateur. Pour plus d'informations sur les ensembles d'autorisations et leur utilisation dans IAM Identity Center, consultezJeux d'autorisations.

Tenez compte des considérations suivantes lors de la création d'ensembles d'autorisations :

- Commencez avec un ensemble d'autorisations prédéfini

  Avec un ensemble d'autorisations prédéfini, qui utilise des autorisations prédéfinies, vous choisissez une seule stratégie AWS gérée parmi la liste des politiques disponibles. Chaque politique accorde un niveau spécifique d'accès aux AWS services et aux ressources ou des autorisations pour une fonction professionnelle commune. Pour plus d'informations sur chacune de ces politiques, consultez la section Politiques AWS gérées pour les fonctions de travail. Après avoir collecté les données d'utilisation, vous pouvez affiner l'ensemble d'autorisations pour le rendre plus restrictif.

- Limiter la durée des sessions de gestion à des périodes de travail raisonnables

  Lorsque les utilisateurs se fédérent dans leur Compte AWS et utilisent la console de AWS gestion ou l'interface de ligne de AWS commande (AWS CLI), IAM Identity Center utilise le paramètre de durée de session indiqué dans le jeu d'autorisations pour contrôler la durée de la session. Lorsque la session utilisateur atteint sa durée de session, il est déconnecté de la console et invité à se reconnecter. Pour des raisons de sécurité, nous vous recommandons de ne pas définir la durée de session au-delà de ce qui est nécessaire pour exécuter le rôle. Par défaut, la valeur de la durée de session est d'une heure. Vous pouvez spécifier une valeur maximale de 12 heures. Pour plus d'informations, consultez Définir la durée de la session.

- Limiter la durée de session du portail utilisateur du personnel

  Les utilisateurs du personnel utilisent les sessions du portail pour choisir les rôles et accéder aux applications. Par défaut, la valeur de la durée maximale de session, qui détermine la durée pendant laquelle un utilisateur du personnel peut se connecter au portail d' AWS accès avant de devoir s'authentifier à nouveau, est de huit heures. Vous pouvez spécifier une valeur maximale de 90 jours. Pour plus d'informations, consultez Configurer la durée de session du portail d' AWS accès et des applications intégrées d'IAM Identity Center.

- Utiliser le rôle qui fournit les autorisations de moindre privilège

  Chaque ensemble d'autorisations que vous créez et attribuez à votre utilisateur apparaît comme un rôle disponible dans le portail AWS d'accès. Lorsque vous vous connectez au portail en tant qu'utilisateur, choisissez le rôle qui correspond à l'ensemble d'autorisations le plus restrictif que vous pouvez utiliser pour effectuer des tâches dans le compte, plutôt que`AdministratorAccess`. Testez vos ensembles d'autorisations pour vérifier qu'ils fournissent l'accès nécessaire avant d'envoyer l'invitation à l'utilisateur.

> **Note**
>
> Vous pouvez également l'utiliser AWS CloudFormationpour créer et attribuer des ensembles d'autorisations et attribuer des utilisateurs à ces ensembles d'autorisations.

Rubriques

Crée un jeu d'autorisations.

Utilisez cette procédure pour créer un ensemble d'autorisations prédéfini qui utilise une seule politique AWS gérée, ou un ensemble d'autorisations personnalisé qui utilise jusqu'à 10 politiques AWS gérées ou gérées par le client et une politique intégrée. Vous pouvez demander un ajustement du nombre maximum de 10 politiques dans la console Service Quotas pour IAM.

Vous pouvez créer un ensemble d'autorisations dans la console IAM Identity Center.

Pour créer un jeu d'autorisations

1. Ouvrez la console IAM Identity Center.
2. Sous Autorisations multi-comptes, choisissez Ensembles d'autorisations.
3. Choisissez Create permission set (Créer un jeu d'autorisations).
4. Sur la page Sélectionner le type d'ensemble d'autorisations, sous Type d'ensemble d'autorisations, sélectionnez un type d'ensemble d'autorisations.
5. Choisissez une ou plusieurs politiques que vous souhaitez utiliser pour l'ensemble d'autorisations, en fonction du type d'ensemble d'autorisations :

   - Ensemble d'autorisations prédéfini

     1. Sous Politique pour un ensemble d'autorisations prédéfini, sélectionnez l'une des politiques de fonction IAM Job ou des politiques d'autorisation communes dans la liste, puis choisissez Next. Pour plus d'informations, consultez les politiques AWS gérées pour les fonctions

de travail et les politiques AWS gérées dans le Guide de AWS Identity and Access Management l'utilisateur.

2. Passez à l'étape 6 pour terminer la page de détails de l'ensemble d'autorisations.

- Ensemble d'autorisations personnalisé

1. Choisissez Suivant.
2. Sur la page Spécifier les politiques et les limites d'autorisation, choisissez les types de politiques IAM que vous souhaitez appliquer à votre nouvel ensemble d'autorisations. Par défaut, vous pouvez ajouter n'importe quelle combinaison d'un maximum de 10 politiques AWS gérées et de politiques gérées par le client à votre ensemble d'autorisations. Ce quota est défini par IAM. Pour l'augmenter, demandez une augmentation du quota IAM. Les politiques gérées associées à un rôle IAM sont associées à un rôle IAM dans la console Service Quotas dans chaque instance à Compte AWS laquelle vous souhaitez attribuer l'ensemble d'autorisations.

   - Développez les politiques AWS gérées pour ajouter des politiques issues d'IAM qui AWS créent et gèrent. Pour plus d'informations, consultez AWS politiques gérées.

     a. Recherchez et choisissez les politiques AWS gérées que vous souhaitez appliquer à vos utilisateurs dans l'ensemble d'autorisations.

     b. Si vous souhaitez ajouter un autre type de politique, choisissez son conteneur et effectuez votre sélection. Choisissez Next lorsque vous avez sélectionné toutes les politiques que vous souhaitez appliquer. Passez à l'étape 6 pour terminer la page de détails de l'ensemble d'autorisations.

   - Développez les politiques gérées par le client pour ajouter des politiques IAM que vous créez et gérez. Pour plus d'informations, consultez Politiques gérées par le client.

     a. Choisissez Joindre des politiques et entrez le nom de la politique que vous souhaitez ajouter à votre ensemble d'autorisations. Dans chaque compte auquel vous souhaitez attribuer l'ensemble d'autorisations, créez une politique portant le nom que vous avez saisi. Il est recommandé d'attribuer les mêmes autorisations à la politique dans chaque compte.

     b. Choisissez Attacher plus pour ajouter une autre politique.

     c. Si vous souhaitez ajouter un autre type de politique, choisissez son conteneur et effectuez votre sélection. Choisissez Next lorsque vous avez sélectionné toutes les politiques que vous souhaitez appliquer. Passez à l'étape 6 pour terminer la page de détails de l'ensemble d'autorisations.

- Développez la politique intégrée pour ajouter un texte de politique personnalisé au format JSON. Les politiques intégrées ne correspondent pas aux ressources IAM existantes. Pour créer une politique intégrée, entrez un langage de politique personnalisé dans le formulaire fourni. IAM Identity Center ajoute la politique aux ressources IAM qu'il crée dans vos comptes membres. Pour plus d'informations, consultez Politiques en ligne.

  a. Ajoutez les actions et les ressources souhaitées dans l'éditeur interactif à votre politique intégrée. Des déclarations supplémentaires peuvent être ajoutées à l'aide de l'option Ajouter une nouvelle déclaration.

  b. Si vous souhaitez ajouter un autre type de politique, choisissez son conteneur et effectuez votre sélection. Choisissez Next lorsque vous avez sélectionné toutes les politiques que vous souhaitez appliquer. Passez à l'étape 6 pour terminer la page de détails de l'ensemble d'autorisations.

- Élargissez la limite des autorisations pour ajouter une politique IAM AWS gérée ou gérée par le client en tant qu'autorisations maximales que vos autres politiques de l'ensemble d'autorisations peuvent attribuer. Pour plus d'informations, consultez Limites d'autorisations.

  a. Choisissez Utiliser une limite d'autorisations pour contrôler le maximum d'autorisations.

  b. Choisissez une politique AWS gérée pour définir une politique d'IAM qui AWScrée et gère comme limite d'autorisations. Choisissez les politiques gérées par le client pour définir une politique à partir d'IAM que vous créez et gérez comme limite d'autorisations.

  c. Si vous souhaitez ajouter un autre type de politique, choisissez son conteneur et effectuez votre sélection. Choisissez Next lorsque vous avez sélectionné toutes les politiques que vous souhaitez appliquer. Passez à l'étape 6 pour terminer la page de détails de l'ensemble d'autorisations.

6. Sur la page Spécifier les détails de l'ensemble d'autorisations, procédez comme suit :

   1. Sous Nom de l'ensemble d'autorisations, tapez un nom pour identifier cet ensemble d'autorisations dans IAM Identity Center. Le nom que vous spécifiez pour cet ensemble d'autorisations apparaît dans le portail AWS d'accès en tant que rôle disponible. Les utilisateurs se connectent AWS au portail d'accès Compte AWS, choisissent un, puis le rôle.
   2. (Facultatif) Vous pouvez également saisir une description. La description apparaît uniquement dans la console IAM Identity Center, et non dans le portail AWS d'accès.

3. (Facultatif) Spécifiez la valeur de la durée de la session. Cette valeur détermine la durée pendant laquelle un utilisateur peut être connecté avant que la console ne le déconnecte de sa session. Pour plus d'informations, consultez Définir la durée de la session.
4. (Facultatif) Spécifiez la valeur de l'état du relais. Cette valeur est utilisée dans le processus de fédération pour rediriger les utilisateurs au sein du compte. Pour plus d'informations, consultez Définir l'état du relais.

   > **Note**
   >
   > L'URL de l'état du relais doit se trouver dans le AWS Management Console. Par exemple :
   > **`https://console.aws.amazon.com/ec2/`**

5. Développez les balises (facultatif), choisissez Ajouter une balise, puis spécifiez les valeurs de clé et de valeur (facultatif).

   Pour plus d'informations sur les balises, consultez Balisage de ressources AWS IAM Identity Center.
6. Choisissez Suivant.
7. Sur la page Réviser et créer, passez en revue les sélections que vous avez effectuées, puis choisissez Créer.
8. Par défaut, lorsque vous créez un ensemble d'autorisations, celui-ci n'est pas provisionné (utilisé dans aucun d'entre eux Comptes AWS). Pour attribuer un ensemble d'autorisations dans un Compte AWS, vous devez attribuer l'accès à IAM Identity Center aux utilisateurs et aux groupes du compte, puis appliquer l'ensemble d'autorisations à ces utilisateurs et groupes. Pour plus d'informations, consultez Accès par authentification unique à Comptes AWS.

Déléguer l'administration des ensembles d'autorisations

IAM Identity Center vous permet de déléguer la gestion des ensembles d'autorisations et des attributions dans les comptes en créant des politiques IAM qui font référence aux Amazon Resource Names (ARN) des ressources IAM Identity Center. Par exemple, vous pouvez créer des politiques qui permettent à différents administrateurs de gérer les attributions dans des comptes spécifiques pour des ensembles d'autorisations dotés de balises spécifiques.

Vous pouvez utiliser l'une des méthodes suivantes pour créer ces types de politiques.

- (Recommandé) Créez des ensembles d'autorisations dans IAM Identity Center, chacun avec une politique différente, et attribuez les ensembles d'autorisations à différents utilisateurs ou groupes. Cela vous permet de gérer les autorisations administratives pour les utilisateurs qui se connectent à l'aide de la source d'identité IAM Identity Center que vous avez choisie.
- Créez des politiques personnalisées dans IAM, puis associez-les aux rôles IAM assumés par vos administrateurs. Pour plus d'informations sur les rôles, consultez la section Rôles IAM pour obtenir les autorisations administratives IAM Identity Center qui leur ont été attribuées.

> **Important**
>
> Les ARN des ressources IAM Identity Center distinguent les majuscules et minuscules.

Ce qui suit montre le cas approprié pour faire référence à l'ensemble d'autorisations IAM Identity Center et aux types de ressources du compte.

Types de ressources	ARN	Clés de contexte
PermissionSet	`arn:${Partition}:sso:::permissionSet/${InstanceId}/${PermissionSetId}`	`aws:ResourceTag/${TagKey}`
Compte	`arn:${Partition}:sso:::account/${AccountId}`	Ne s'applique pas

Utiliser les politiques IAM dans les ensembles d'autorisations

DansCrée un jeu d'autorisations., vous avez appris à ajouter des politiques, notamment des politiques gérées par le client et des limites d'autorisations, à un ensemble d'autorisations. Lorsque vous ajoutez des politiques et des autorisations gérées par le client à un ensemble d'autorisations, IAM Identity Center ne crée aucune Comptes AWS politique. Vous devez plutôt créer ces politiques à l'avance dans chaque compte auquel vous souhaitez attribuer votre ensemble d'autorisations, et les faire correspondre au nom et aux spécifications de chemin de votre ensemble d'autorisations. Lorsque vous attribuez un ensemble d'autorisations Compte AWS à un membre de

votre organisation, IAM Identity Center crée un rôle AWS Identity and Access Management (IAM) et associe vos politiques IAM à ce rôle.

> **Note**
>
> Avant d'attribuer votre ensemble d'autorisations aux politiques IAM, vous devez préparer votre compte de membre. Le nom d'une politique IAM dans votre compte membre doit correspondre au nom de la politique dans votre compte de gestion en distinguant majuscules et minuscules. IAM Identity Center ne parvient pas à attribuer l'ensemble d'autorisations si la politique n'existe pas dans votre compte de membre.
> Les autorisations accordées par la politique ne doivent pas nécessairement correspondre exactement aux différents comptes.

Pour attribuer une politique IAM à un ensemble d'autorisations

1. Créez une politique IAM dans chacun des Comptes AWS endroits où vous souhaitez attribuer l'ensemble d'autorisations.
2. Attribuez des autorisations à la politique IAM. Vous pouvez attribuer différentes autorisations à différents comptes. Pour une expérience cohérente, configurez et maintenez des autorisations identiques dans chaque politique. Vous pouvez utiliser des ressources d'automatisation telles que AWS CloudFormation StackSets la création de copies d'une politique IAM portant le même nom et les mêmes autorisations dans chaque compte membre. Pour plus d'informations à ce sujet CloudFormation StackSets, consultez la section Travailler avec AWS CloudFormation StackSets dans le guide de AWS CloudFormation l'utilisateur.
3. Créez un ensemble d'autorisations dans votre compte de gestion et ajoutez votre politique IAM sous Politiques gérées par le client ou Limite des autorisations. Pour plus de détails sur la création d'un ensemble d'autorisations, voirCrée un jeu d'autorisations..
4. Ajoutez les politiques intégrées, les politiques AWS gérées ou les politiques IAM supplémentaires que vous avez préparées.
5. Créez et attribuez votre ensemble d'autorisations.

Supprimer des ensembles d'autorisations

Si vous souhaitez révoquer une session d'ensemble d'autorisations active, consultezRévoquer les sessions de rôle IAM actives créées par des ensembles d'autorisations.

Avant de pouvoir supprimer un ensemble d'autorisations d'IAM Identity Center, vous devez le supprimer de tous Comptes AWS ceux qui l'utilisent. Pour vérifier l'accès des utilisateurs et des groupes existants, voirAfficher les attributions des utilisateurs et des groupes.

Pour supprimer un ensemble d'autorisations d'un Compte AWS

1. Ouvrez la console IAM Identity Center.
2. Sous Autorisations multi-comptes, choisissez Comptes AWS.
3. Sur la Comptes AWSpage, une liste arborescente de votre organisation apparaît. Sélectionnez le nom du groupe Compte AWS d'autorisations dont vous souhaitez supprimer l'ensemble d'autorisations.
4. Sur la page d'aperçu du Compte AWS, choisissez l'onglet Ensembles d'autorisations.
5. Cochez la case à côté de l'ensemble d'autorisations que vous souhaitez supprimer, puis choisissez Supprimer.
6. Dans la boîte de dialogue Supprimer l'ensemble d'autorisations, vérifiez que le bon ensemble d'autorisations est sélectionné, tapez **`Delete`** pour confirmer la suppression, puis choisissez Supprimer l'accès.

Suivez la procédure ci-dessous pour supprimer un ou plusieurs ensembles d'autorisations afin qu'aucun membre de l'organisation ne puisse plus Compte AWS les utiliser.

> **Note**
>
> Tous les utilisateurs et groupes auxquels cet ensemble d'autorisations a été attribué, quel que Compte AWS soit l'utilisateur qui l'utilise, ne pourront plus se connecter. Pour vérifier l'accès des utilisateurs et des groupes existants, voirAfficher les attributions des utilisateurs et des groupes.

Pour supprimer un ensemble d'autorisations d'un Compte AWS

1. Ouvrez la console IAM Identity Center.
2. Sous Autorisations multi-comptes, choisissez Ensembles d'autorisations.
3. Sélectionnez l'ensemble d'autorisations que vous souhaitez supprimer, puis choisissez Supprimer.

4. Dans la boîte de dialogue Supprimer l'ensemble d'autorisations, tapez le nom du jeu d'autorisations pour confirmer la suppression, puis choisissez Supprimer. Le nom est sensible à la casse.

Configurer les propriétés des ensembles d'autorisations

Dans IAM Identity Center, vous pouvez personnaliser l'expérience utilisateur en configurant les propriétés du jeu d'autorisations suivantes.

Rubriques

Définir la durée de la session

Pour chaque ensemble d'autorisations, vous pouvez spécifier une durée de session afin de contrôler la durée pendant laquelle un utilisateur peut être connecté à un Compte AWS. Lorsque la durée spécifiée est écoulée, AWS déconnecte l'utilisateur de la session.

Lorsque vous créez un nouvel ensemble d'autorisations, la durée de la session est fixée à 1 heure (en secondes) par défaut. La durée minimale de la session est d'une heure et peut être fixée à un maximum de 12 heures. IAM Identity Center crée automatiquement des rôles IAM dans chaque compte attribué pour chaque ensemble d'autorisations, et configure ces rôles avec une durée de session maximale de 12 heures.

Lorsque les utilisateurs se fédèrent dans leur Compte AWS console ou lorsque le AWS Command Line Interface (AWS CLI) est utilisé, IAM Identity Center utilise le paramètre de durée de session figurant sur le jeu d'autorisations pour contrôler la durée de la session. Par défaut, les rôles IAM générés par IAM Identity Center pour les ensembles d'autorisations ne peuvent être assumés que par les utilisateurs d'IAM Identity Center, ce qui garantit que la durée de session spécifiée dans le jeu d'autorisations IAM Identity Center est appliquée.

> **Important**
>
> Comme bonne pratique de sécurité, nous vous recommandons de ne pas définir une durée de la session plus longue que ce qui est nécessaire pour exécuter le rôle.

Après avoir créé un ensemble d'autorisations, vous pouvez le mettre à jour pour appliquer une nouvelle durée de session. Utilisez la procédure suivante pour modifier la durée de session d'un ensemble d'autorisations.

Pour définir la durée de session

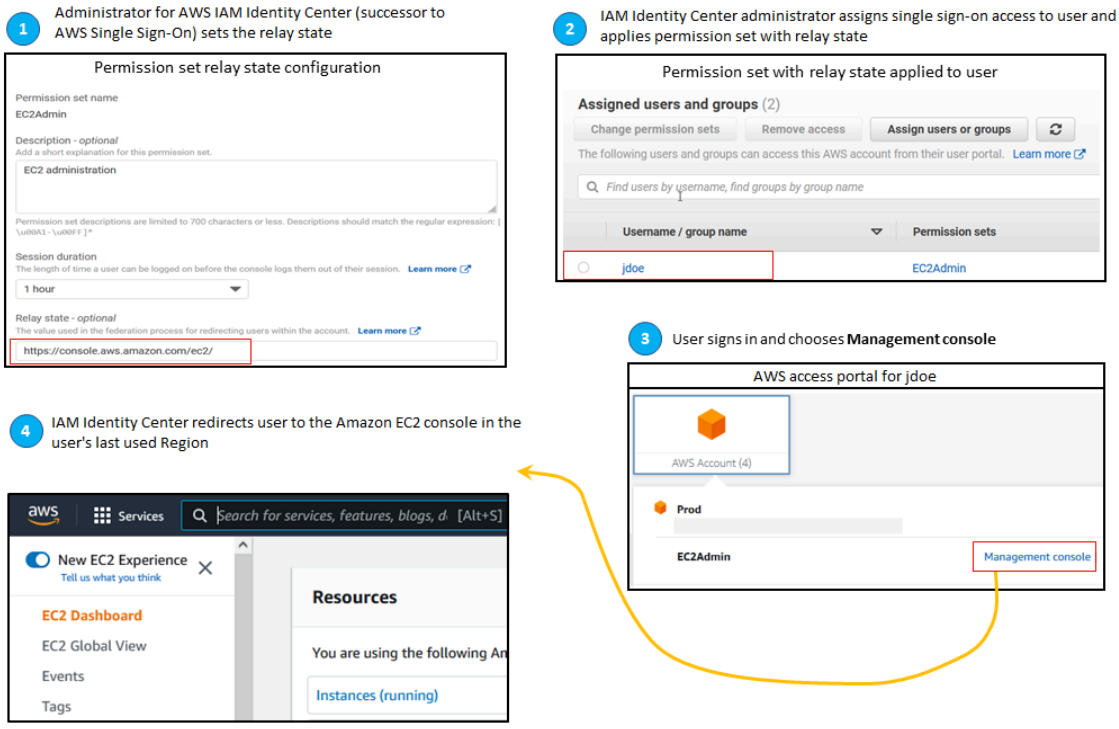
1. Ouvrez la console IAM Identity Center.
2. Sous Autorisations multi-comptes, choisissez Ensembles d'autorisations.
3. Choisissez le nom de l'ensemble d'autorisations dont vous souhaitez modifier la durée de session.
4. Sur la page de détails de l'ensemble d'autorisations, à droite de l'en-tête de la section Paramètres généraux, choisissez Modifier.
5. Sur la page Modifier les paramètres généraux de l'ensemble d'autorisations, choisissez une nouvelle valeur pour la durée de la session.
6. Si l'ensemble d'autorisations est provisionné dans l'un d'entre Comptes AWS eux, les noms des comptes apparaissent sous Comptes AWS pour être réapprovisionnés automatiquement. Une fois que la valeur de durée de session pour l'ensemble d'autorisations est mise à jour, tous Comptes AWS ceux qui utilisent l'ensemble d'autorisations sont reprovisionnés. Cela signifie que la nouvelle valeur de ce paramètre est appliquée à tous ceux Comptes AWS qui utilisent l'ensemble d'autorisations.
7. Sélectionnez Enregistrer les modifications.
8. En haut de la Comptes AWSpage, une notification apparaît.

   - Si l'ensemble d'autorisations est fourni dans un ou plusieurs comptes Comptes AWS, la notification confirme qu' Comptes AWS ils ont été reprovisionnés avec succès et que le jeu d'autorisations mis à jour a été appliqué aux comptes.
   - Si l'ensemble d'autorisations n'est pas fourni dans un Compte AWS, la notification confirme que les paramètres du jeu d'autorisations ont été mis à jour.

Définir l'état du relais

Par défaut, lorsqu'un utilisateur se connecte au portail d' AWS accès, choisit un compte, puis choisit le rôle AWS créé à partir de l'ensemble d'autorisations attribué, IAM Identity Center redirige le navigateur de l'utilisateur vers le. AWS Management Console Vous pouvez modifier ce comportement en définissant l'état du relais sur une autre URL de console. La définition de l'état du relais vous permet de fournir à l'utilisateur un accès rapide à la console la mieux adaptée à son rôle.

Par exemple, vous pouvez définir l'état du relais sur l'URL de la console Amazon EC2 (**`https://console.aws.amazon.com/ec2/`**) pour rediriger l'utilisateur vers cette console lorsqu'il choisit le rôle d'administrateur Amazon EC2. Lors de la redirection vers l'URL par défaut ou vers l'URL de l'état du relais, IAM Identity Center achemine le navigateur de l'utilisateur vers le point de terminaison de la console Région AWS utilisé pour la dernière fois par l'utilisateur. Par exemple, si un utilisateur a mis fin à sa dernière session de console dans la région Europe (Stockholm) (eu-north-1), il est redirigé vers la console Amazon EC2 de cette région.



Pour configurer IAM Identity Center afin de rediriger l'utilisateur vers une console dans un environnement spécifique Région AWS, incluez la spécification de région dans l'URL. Par exemple, pour rediriger l'utilisateur vers la console Amazon EC2 dans la région USA Est (Ohio) (us-east-2), spécifiez l'URL de la console Amazon EC2 dans cette région (). **`https://us-east-2.console.aws.amazon.com/ec2/`** Si vous avez activé le centre d'identité IAM dans la région USA Ouest (Oregon) (us-west-2) et que vous souhaitez rediriger l'utilisateur vers cette région, spécifiez-le. **`https://us-west-2.console.aws.amazon.com`**

Utilisez la procédure suivante pour configurer l'URL de l'état du relais pour un ensemble d'autorisations.

Pour configurer l'état du relais

1. Ouvrez la console IAM Identity Center.
2. Sous Autorisations multi-comptes, choisissez Ensembles d'autorisations.
3. Choisissez le nom de l'ensemble d'autorisations pour lequel vous souhaitez définir la nouvelle URL de l'état du relais.
4. Sur la page de détails de l'ensemble d'autorisations, à droite de l'en-tête de la section Paramètres généraux, choisissez Modifier.
5. Sur la page Modifier les paramètres généraux de l'ensemble d'autorisations, sous État du relais, tapez une URL de console pour l'un des AWS services. Par exemple :

   `https://console.aws.amazon.com/ec2/`

   > **Note**
   >
   > L'URL de l'état du relais doit se trouver dans le AWS Management Console.

6. Si l'ensemble d'autorisations est provisionné dans l'un d'entre Comptes AWS eux, les noms des comptes apparaissent sous Comptes AWS pour être réapprovisionnés automatiquement. Une fois que l'URL de l'état du relais pour l'ensemble d'autorisations est mise à jour, tous Comptes AWS ceux qui utilisent l'ensemble d'autorisations sont reprovisionnés. Cela signifie que la nouvelle valeur de ce paramètre est appliquée à tous ceux Comptes AWS qui utilisent l'ensemble d'autorisations.
7. Sélectionnez Enregistrer les modifications.
8. En haut de la page AWS Organisation, une notification apparaît.

   - Si l'ensemble d'autorisations est fourni dans un ou plusieurs comptes Comptes AWS, la notification confirme qu' Comptes AWS ils ont été reprovisionnés avec succès et que le jeu d'autorisations mis à jour a été appliqué aux comptes.
   - Si l'ensemble d'autorisations n'est pas fourni dans un Compte AWS, la notification confirme que les paramètres du jeu d'autorisations ont été mis à jour.

> **Note**
>
> Vous pouvez automatiser ce processus à l'aide de l' AWS API, d'un AWS SDK ou du AWS Command Line Interface(AWS CLI). Pour plus d'informations, consultez :

- Les `UpdatePermissionSet` actions `CreatePermissionSet` ou contenues dans la référence d'API IAM Identity Center
- Les `update-permission-set` commandes `create-permission-set` ou dans la sso-adminsection de la référence des AWS CLI commandes.

Utiliser une politique de refus pour révoquer les autorisations des utilisateurs actifs

Il se peut que vous deviez révoquer l'accès d'un utilisateur à IAM Identity Center Comptes AWS alors que celui-ci utilise activement un ensemble d'autorisations. Vous pouvez les empêcher d'utiliser leurs sessions de rôle IAM actives en implémentant à l'avance une politique de refus pour un utilisateur non spécifié, puis si nécessaire, vous pouvez mettre à jour la politique de refus pour spécifier l'utilisateur dont vous souhaitez bloquer l'accès. Cette rubrique explique comment créer une politique de refus et explique comment déployer la politique.

Préparez-vous à révoquer une session de rôle IAM active créée par un ensemble d'autorisations

Vous pouvez empêcher l'utilisateur de prendre des mesures avec un rôle IAM qu'il utilise activement en appliquant une politique de refus de tout à un utilisateur spécifique par le biais d'une politique de contrôle des services. Vous pouvez également empêcher un utilisateur d'utiliser un ensemble d'autorisations tant que vous n'avez pas modifié son mot de passe, ce qui permet de supprimer un mauvais acteur utilisant activement des informations d'identification volées à mauvais escient. Si vous devez refuser l'accès de manière générale et empêcher un utilisateur de saisir à nouveau un ensemble d'autorisations ou d'accéder à d'autres ensembles d'autorisations, vous pouvez également supprimer tous les accès des utilisateurs, arrêter la session active du portail d' AWS accès et désactiver la connexion de l'utilisateur. Consultez Révoquer les sessions de rôle IAM actives créées par des ensembles d'autorisations pour savoir comment utiliser la politique de refus en conjonction avec des actions supplémentaires pour une révocation d'accès plus large.

Politique de refus

Vous pouvez utiliser une politique de refus assortie d'une condition correspondant à celle `UserID` de l'utilisateur figurant dans la banque d'identités IAM Identity Center afin d'empêcher d'autres actions d'un rôle IAM que l'utilisateur utilise activement. L'utilisation de cette politique permet d'éviter tout impact sur les autres utilisateurs susceptibles d'utiliser le même ensemble d'autorisations lorsque vous déployez la politique de refus. Cette politique utilise l'identifiant utilisateur fictif. Pour `"identitystore:userId"` cela *`Add user ID here`*, vous allez le mettre à jour avec le nom d'utilisateur pour lequel vous souhaitez révoquer l'accès.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "*"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "identitystore:userId": "Add user ID here"
                }
            }
        }
    ]
}
```

Bien que vous puissiez utiliser une autre clé de condition“`aws:userId`”, telle que, elle “`identitystore:userId`” est certaine, car il s'agit d'une valeur unique au monde associée à une personne. L'utilisation “`aws:userId`” dans cette condition peut être affectée par la façon dont les attributs utilisateur sont synchronisés à partir de votre source d'identités et peut changer si le nom d'utilisateur ou l'adresse e-mail de l'utilisateur changent.

Dans la console IAM Identity Center, vous pouvez trouver celui d'un utilisateur `identitystore:userId` en accédant à Utilisateurs, en recherchant l'utilisateur par son nom, en développant la section Informations générales et en copiant l'ID utilisateur. Il est également pratique d'arrêter la session du portail d' AWS accès d'un utilisateur et de désactiver son accès de connexion dans la même section lors de la recherche de son nom d'utilisateur. Vous pouvez automatiser le processus de création d'une politique de refus en obtenant l'ID utilisateur de l'utilisateur en interrogeant les API du magasin d'identités.

Déploiement de la politique de refus

Vous pouvez utiliser un identifiant utilisateur fictif qui n'est pas valide, par exemple pour déployer la politique de refus à l'avance à l'aide d'une politique de contrôle des services (SCP) que vous attachez aux Comptes AWS utilisateurs susceptibles d'avoir accès. *`Add user ID here`* C'est l'approche recommandée pour sa facilité et sa rapidité d'impact. Lorsque vous révoquez l'accès d'un utilisateur à l'aide de la politique de refus, vous modifiez la politique pour remplacer l'ID utilisateur fictif par l'ID utilisateur de la personne dont vous souhaitez révoquer l'accès. Cela empêche l'utilisateur

d'effectuer des actions avec les autorisations définies dans chaque compte auquel vous associez le SCP. Il bloque les actions de l'utilisateur même s'il utilise sa session de portail AWS d'accès active pour accéder à différents comptes et assumer différents rôles. L'accès de l'utilisateur étant totalement bloqué par le SCP, vous pouvez alors désactiver sa capacité à se connecter, révoquer ses attributions et arrêter sa session sur le portail AWS d'accès si nécessaire.

Au lieu d'utiliser des SCP, vous pouvez également inclure la politique de refus dans la politique intégrée des ensembles d'autorisations et dans les politiques gérées par le client qui sont utilisées par les ensembles d'autorisations auxquels l'utilisateur peut accéder.

Si vous devez révoquer l'accès à plusieurs personnes, vous pouvez utiliser une liste de valeurs dans le bloc de conditions, telles que :

```
        "Condition": {
                "StringEquals": {
                    "identitystore:userId": [" user1 userId", "user2 userId"...]
                    }
    }
```

> **Important**
>
> Quelle que soit la ou les méthodes que vous utilisez, vous devez prendre toute autre mesure corrective et conserver le nom d'utilisateur de l'utilisateur dans la politique pendant au moins 12 heures. Passé ce délai, tous les rôles assumés par l'utilisateur expirent et vous pouvez alors supprimer son ID utilisateur de la politique de refus.

Référencement des ensembles d'autorisations dans les politiques de ressources, Amazon EKS et AWS KMS

Lorsque vous attribuez un ensemble d'autorisations à un AWS compte, IAM Identity Center crée un rôle dont le nom commence `AWSReservedSSO_` par.

Le nom complet et le nom Amazon Resource Name (ARN) du rôle utilisent le format suivant :

Nom	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*

Par exemple, si vous créez un ensemble d'autorisations qui accorde l'accès au AWS compte aux administrateurs de base de données, un rôle correspondant est créé avec le nom et l'ARN suivants :

Nom	ARN
AWSReservedSSO_DatabaseAdministrator_1234567890abcdef	arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_DatabaseAdministrator_1234567890abcdef

Si vous supprimez toutes les attributions associées à cet ensemble d'autorisations dans le AWS compte, le rôle correspondant créé par IAM Identity Center est également supprimé. Si vous attribuez ultérieurement une nouvelle attribution au même ensemble d'autorisations, IAM Identity Center crée un nouveau rôle pour le jeu d'autorisations. Le nom et l'ARN du nouveau rôle incluent un suffixe différent et unique. Dans cet exemple, le suffixe unique est abcdef0123456789.

Nom	ARN
AWSReservedSSO_DatabaseAdministrator_ **abcdef0123456789**	arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_DatabaseAdministrator_ **abcdef0123456789**

La modification du suffixe du nouveau nom et du nouveau ARN du rôle entraînera la création de toutes les politiques faisant référence au nom et à l'ARN d'origine out-of-date, ce qui perturbera l'accès des personnes utilisant l'ensemble d'autorisations correspondant. Par exemple, une modification de l'ARN du rôle perturbera l'accès des utilisateurs à l'ensemble d'autorisations si l'ARN d'origine est référencé dans les configurations suivantes :

- Dans le `aws-auth ConfigMap` fichier d'Amazon Elastic Kubernetes Service (Amazon EKS)
- Dans une politique basée sur les ressources pour une clé AWS Key Management Service (AWS KMS). Cette politique est également appelée politique clé.

Bien que vous puissiez mettre à jour les politiques basées sur les ressources pour la plupart AWS des services afin de faire référence à un nouvel ARN pour un rôle correspondant à un ensemble d'autorisations, vous devez avoir un rôle de sauvegarde que vous devez créer dans IAM pour Amazon EKS et si AWS KMS l'ARN change. Pour Amazon EKS, le rôle IAM de sauvegarde doit exister dans le`aws-auth ConfigMap`. Car AWS KMS elle doit figurer dans vos politiques clés. Si vous ne disposez d'aucun rôle IAM de secours dans les deux cas, vous devez contacter AWS Support.

Recommandations pour éviter les interruptions d'accès

Pour éviter les interruptions d'accès dues à des modifications de l'ARN d'un rôle correspondant à un ensemble d'autorisations, nous vous recommandons de procéder comme suit.

- Conservez au moins une attribution d'ensemble d'autorisations.

  Conservez cette attribution dans les AWS comptes qui contiennent les rôles auxquels vous faites référence dans le `aws-auth ConfigMap` cas d'Amazon EKS, les politiques clés dans AWS KMS Amazon EKS ou les politiques basées sur les ressources pour les autres. Services AWS

  Par exemple, si vous créez un ensemble d'`EKSAccess`autorisations et que vous référencez l'ARN du rôle correspondant à partir du AWS compte`111122223333`, attribuez définitivement un groupe administratif au jeu d'autorisations de ce compte. L'attribution étant permanente, IAM Identity Center ne supprimera pas le rôle correspondant, ce qui élimine le risque de changement de nom. Le groupe administratif y aura toujours accès sans risque d'augmentation de privilèges.
- Pour Amazon EKS et AWS KMS : incluez un rôle créé dans IAM.

  Si vous faites référence à des ARN de rôles pour des ensembles d'autorisations dans un `aws-auth ConfigMap` cluster Amazon EKS ou dans des politiques AWS KMS clés relatives aux clés,

nous vous recommandons d'inclure également au moins un rôle que vous créez dans IAM. Le rôle doit vous permettre d'accéder au cluster Amazon EKS ou de gérer la politique AWS KMS clé. L'ensemble d'autorisations doit être en mesure d'assumer ce rôle. Ainsi, si l'ARN du rôle d'un ensemble d'autorisations change, vous pouvez mettre à jour la référence à l'ARN dans la politique AWS KMS clé `aws-auth ConfigMap` or. La section suivante fournit un exemple de la manière dont vous pouvez créer une politique de confiance pour un rôle créé dans IAM. Le rôle ne peut être assumé que par un ensemble d'`AdministratorAccess`autorisations.

Exemple de politique de confiance personnalisée

Voici un exemple de politique de confiance personnalisée qui fournit un ensemble d'`AdministratorAccess`autorisations permettant d'accéder à un rôle créé dans IAM. Les principaux éléments de cette politique sont les suivants :

- L'élément principal de cette politique de confiance spécifie un principal de AWS compte. Dans cette politique, les responsables du AWS compte `111122223333` disposant d'`sts:AssumeRole`autorisations peuvent assumer le rôle créé dans IAM.
- Cette politique `Condition element` de confiance définit des exigences supplémentaires pour les principaux qui peuvent assumer le rôle créé dans IAM. Dans cette politique, l'ensemble d'autorisations avec le rôle ARN suivant peut assumer le rôle.

```
arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/
AWSReservedSSO_AdministratorAccess_*"
```

> **Note**
>
> L'`Condition`élément inclut l'opérateur de `ArnLike` condition et utilise un caractère générique à la fin de l'ARN du rôle défini d'autorisations, plutôt qu'un suffixe unique. Cela signifie que la politique permet à l'ensemble d'autorisations d'assumer le rôle créé dans IAM même si l'ARN du rôle pour l'ensemble d'autorisations change.

```
{
  "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_*"
        }
      }
    }
  ]
}
```

L'inclusion d'un rôle que vous créez dans IAM dans une telle politique vous fournira un accès d'urgence à vos clusters Amazon EKS ou à d'autres AWS ressources si un ensemble d'autorisations ou toutes les attributions à l'ensemble d'autorisations sont accidentellement supprimés et recréés. AWS KMS keys

Contrôle d'accès basé sur les attributs

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit des autorisations en fonction des attributs. Vous pouvez utiliser IAM Identity Center pour gérer l'accès à vos AWS ressources sur plusieurs sites à Comptes AWS l'aide d'attributs utilisateur provenant de n'importe quelle source d'identité IAM Identity Center. Dans AWS, ces attributs sont appelés balises. L'utilisation des attributs utilisateur sous forme de balises vous AWS permet de simplifier le processus de création d'autorisations précises AWS et de garantir que votre personnel n'a accès qu'aux AWS ressources associées aux balises correspondantes.

Par exemple, vous pouvez attribuer aux développeurs Bob et Sally, issus de deux équipes différentes, le même ensemble d'autorisations dans IAM Identity Center, puis sélectionner l'attribut du nom de l'équipe pour le contrôle d'accès. Lorsque Bob et Sally se connectent à leur Comptes AWS, IAM Identity Center envoie leur attribut de nom d'équipe dans la AWS session afin que Bob et Sally puissent accéder aux ressources AWS du projet uniquement si leur attribut de nom d'équipe correspond au tag de nom d'équipe figurant sur la ressource du projet. Si Bob rejoint l'équipe de Sally à l'avenir, vous pouvez modifier son accès en mettant simplement à jour son attribut de nom d'équipe dans le répertoire de l'entreprise. La prochaine fois que Bob se connectera, il aura automatiquement accès aux ressources de projet de sa nouvelle équipe sans avoir à mettre à jour les autorisations AWS.

Cette approche permet également de réduire le nombre d'autorisations distinctes que vous devez créer et gérer dans IAM Identity Center, car les utilisateurs associés aux mêmes ensembles d'autorisations peuvent désormais disposer d'autorisations uniques en fonction de leurs attributs. Vous pouvez utiliser ces attributs utilisateur dans les ensembles d'autorisations et les politiques basées sur les ressources d'IAM Identity Center pour implémenter ABAC dans les AWS ressources et simplifier la gestion des autorisations à grande échelle.

Avantages

Les avantages supplémentaires de l'utilisation d'ABAC dans IAM Identity Center sont les suivants.

- ABAC nécessite moins d'ensembles d'autorisations : comme vous n'avez pas à créer de politiques différentes pour les différentes fonctions, vous créez moins d'ensembles d'autorisations. Cela réduit la complexité de la gestion des autorisations.
- Grâce à ABAC, les équipes peuvent évoluer et se développer rapidement : les autorisations pour les nouvelles ressources sont automatiquement accordées en fonction des attributs lorsque les ressources sont correctement étiquetées lors de leur création.
- Utilisez les attributs des employés de votre annuaire d'entreprise avec ABAC : vous pouvez utiliser les attributs des employés existants provenant de n'importe quelle source d'identité configurée dans IAM Identity Center pour prendre des décisions de contrôle d'accès dans. AWS
- Suivez qui accède aux ressources — Les administrateurs de sécurité peuvent facilement déterminer l'identité d'une session en examinant les attributs des utilisateurs AWS CloudTrail pour suivre leur activité AWS.

Pour plus d'informations sur la configuration d'ABAC à l'aide de la console IAM Identity Center, consultez. Attributs pour le contrôle d'accès Pour plus d'informations sur l'activation et la configuration d'ABAC à l'aide des API IAM Identity Center, consultez le Guide de CreateInstanceAccessControlAttributeConfigurationréférence des API IAM Identity Center.

Rubriques

- Liste de contrôle : Configuration d'ABAC à AWS l'aide d'IAM Identity Center
- Attributs pour le contrôle d'accès

Liste de contrôle : Configuration d'ABAC à AWS l'aide d'IAM Identity Center

Cette liste de contrôle inclut les tâches de configuration nécessaires pour préparer vos AWS ressources et configurer IAM Identity Center pour l'accès ABAC. Effectuez les tâches de cette liste de contrôle dans l'ordre. Lorsqu'un lien de référence vous amène à un sujet, revenez à ce sujet afin de pouvoir effectuer les tâches restantes de cette liste de contrôle.

Étape	Tâche	Référence
1	Découvrez comment ajouter des balises à toutes vos AWS ressources. Pour implémenter ABAC dans IAM Identity Center, vous devez d'abord ajouter des balises à toutes les AWS ressources pour lesquelles vous souhaitez implémenter ABAC.	• Ressources de balisage AWS
2	Découvrez comment configurer votre source d'identité dans IAM Identity Center avec les identités utilisateur et les attributs associés dans votre magasin d'identités. IAM Identity Center vous permet d'utiliser les attributs utilisateur de n'importe quelle source d'identité IAM Identity Center prise en charge pour ABAC in. AWS	• Gérez votre source d'identité
3	Sur la base des critères suivants, déterminez les attributs que vous souhaitez utiliser pour prendre des décisions en matière de contrôle d'accès AWS et envoyez-les à IAM Identity Center.	• Premiers pas
	• Si vous utilisez un fournisseur d'identité (IdP) externe, décidez si vous souhaitez utiliser les attributs transmis par l'IdP ou sélectionner des attributs depuis IAM Identity Center.	• Choix des attributs lors de l'utilisation d'un fournisseur d'identité externe comme source d'identité
	• Si vous choisissez que votre IdP envoie des attributs , configurez votre IdP pour transmettre les attributs dans des assertions SAML. Consultez les `Optional` sections du didacticiel correspondant à votre IdP spécifique.	• Tutoriels de mise en route

Étape	Tâche	Référence
	• Si vous utilisez un IdP comme source d'identité et que vous choisissez de sélectionner des attributs dans IAM Identity Center, étudiez comment configure r le SCIM afin que les valeurs des attributs provienne nt de votre IdP. Si vous ne pouvez pas utiliser SCIM avec votre IdP, ajoutez les utilisateurs et leurs attributs à l'aide de la page utilisateur de la console IAM Identity Center.	• Approvisionnement automatique • Attributs du fournisseur d'identité externe pris en charge
	• Si vous utilisez Active Directory ou IAM Identity Center comme source d'identité, ou si vous utilisez un IdP et choisissez de sélectionner des attributs dans IAM Identity Center, passez en revue les attributs disponibles que vous pouvez configure r. Passez ensuite immédiatement à l'étape 4 pour commencer à configurer vos attributs ABAC à l'aide de la console IAM Identity Center.	• Choix des attributs lors de l'utilisation d'IAM Identity Center comme source d'identité • Choix des attributs lorsque vous AWS Managed Microsoft AD les utilisez comme source d'identité • Mappages par défaut
4	Sélectionnez les attributs à utiliser pour ABAC à l'aide de la page Attributs pour le contrôle d'accès de la console IAM Identity Center. Sur cette page, vous pouvez sélectionner des attributs pour le contrôle d'accès à partir de la source d'identité que vous avez configurée à l'étape 2. Une fois que vos identités et leurs attributs se trouvent dans IAM Identity Center, vous devez créer des paires clé-valeur (mappages) qui vous seront transmises Comptes AWS pour être utilisées dans les décisions de contrôle d'accès.	• Activer et configurer les attributs pour le contrôle d'accès

Étape	Tâche	Référence
5	Créez des politiques d'autorisation personnalisées au sein de votre ensemble d'autorisations et utilisez les attributs de contrôle d'accès pour créer des règles ABAC afin que les utilisateurs puissent uniquemen t accéder aux ressources dont les balises correspon dent. Les attributs utilisateur que vous avez configuré s à l'étape 4 sont utilisés comme balises AWS pour les décisions de contrôle d'accès. Vous pouvez faire référence aux attributs de contrôle d'accès dans la politique d'autorisation à l'aide de la `aws:Princ ipalTag/key` condition.	• Création de politiques d'autorisation pour ABAC dans IAM Identity Center
6	Dans vos différents Comptes AWS, assignez des utilisateurs aux ensembles d'autorisations que vous avez créés à l'étape 5. Cela garantit que lorsqu'ils se fédérent dans leurs comptes et accèdent aux AWS ressources, ils n'y accèdent qu'en fonction des balises correspondantes.	• Attribuer un accès utilisateur à Comptes AWS

Une fois ces étapes terminées, les utilisateurs qui se fédérent pour Compte AWS utiliser l'authentification unique auront accès à leurs AWS ressources en fonction des attributs correspondants.

Attributs pour le contrôle d'accès

Attributs pour le contrôle d'accès est le nom de la page de la console IAM Identity Center où vous sélectionnez les attributs utilisateur que vous souhaitez utiliser dans les politiques pour contrôler l'accès aux ressources. Vous pouvez affecter des utilisateurs à des charges de travail en AWS fonction des attributs existants dans la source d'identité des utilisateurs.

Supposons, par exemple, que vous souhaitiez attribuer l'accès aux compartiments S3 en fonction des noms des départements. Sur la page Attributs pour le contrôle d'accès, vous sélectionnez l'attribut utilisateur du département à utiliser avec le contrôle d'accès basé sur les attributs (ABAC). Dans l'ensemble d'autorisations IAM Identity Center, vous rédigez ensuite une politique qui accorde l'accès aux utilisateurs uniquement lorsque l'attribut Department correspond à la balise de département que

vous avez attribuée à vos compartiments S3. IAM Identity Center transmet l'attribut de département de l'utilisateur au compte auquel il accède. L'attribut est ensuite utilisé pour déterminer l'accès en fonction de la politique. Pour plus d'informations sur ABAC, consultezContrôle d'accès basé sur les attributs.

Premiers pas

La manière dont vous commencez à configurer les attributs pour le contrôle d'accès dépend de la source d'identité que vous utilisez. Quelle que soit la source d'identité que vous choisissez, après avoir sélectionné vos attributs, vous devez créer ou modifier les politiques relatives aux ensembles d'autorisations. Ces politiques doivent accorder aux identités des utilisateurs l'accès aux AWS ressources.

Choix des attributs lors de l'utilisation d'IAM Identity Center comme source d'identité

Lorsque vous configurez IAM Identity Center comme source d'identité, vous devez d'abord ajouter des utilisateurs et configurer leurs attributs. Accédez ensuite à la page Attributs pour le contrôle d'accès et sélectionnez les attributs que vous souhaitez utiliser dans les politiques. Enfin, accédez à la Comptes AWSpage pour créer ou modifier des ensembles d'autorisations afin d'utiliser les attributs d'ABAC.

Choix des attributs lorsque vous AWS Managed Microsoft AD les utilisez comme source d'identité

Lorsque vous configurez IAM Identity Center AWS Managed Microsoft AD comme source d'identité, vous mappez d'abord un ensemble d'attributs d'Active Directory aux attributs utilisateur d'IAM Identity Center. Accédez ensuite à la page Attributs pour le contrôle d'accès. Choisissez ensuite les attributs à utiliser dans votre configuration ABAC en fonction de l'ensemble existant d'attributs SSO mappés depuis Active Directory. Enfin, créez des règles ABAC en utilisant les attributs de contrôle d'accès dans les ensembles d'autorisations pour accorder aux identités des utilisateurs l'accès aux AWS ressources. Pour obtenir la liste des mappages par défaut des attributs utilisateur dans IAM Identity Center avec les attributs utilisateur de votre AWS Managed Microsoft AD annuaire, consultez. Mappages par défaut

Choix des attributs lors de l'utilisation d'un fournisseur d'identité externe comme source d'identité

Lorsque vous configurez IAM Identity Center avec un fournisseur d'identité externe (IdP) comme source d'identité, il existe deux manières d'utiliser les attributs pour ABAC.

- Vous pouvez configurer votre IdP pour envoyer les attributs via des assertions SAML. Dans ce cas, IAM Identity Center transmet le nom et la valeur de l'attribut de l'IdP à des fins d'évaluation des politiques.

  > **Note**
  >
  > Les attributs des assertions SAML ne seront pas visibles sur la page Attributs pour le contrôle d'accès. Vous devez connaître ces attributs à l'avance et les ajouter aux règles de contrôle d'accès lorsque vous créez des politiques. Si vous décidez de faire confiance à votre externe IdPs pour les attributs, ces attributs seront toujours transmis lorsque les utilisateurs se fédéreront dans Comptes AWS. Dans les scénarios où les mêmes attributs arrivent à IAM Identity Center via SAML et SCIM, la valeur des attributs SAML a priorité dans les décisions de contrôle d'accès.

- Vous pouvez configurer les attributs que vous utilisez depuis la page Attributs pour le contrôle d'accès de la console IAM Identity Center. Les valeurs d'attributs que vous choisissez ici remplacent les valeurs de tous les attributs correspondants provenant d'un IdP via une assertion. Selon que vous utilisez ou non le SCIM, tenez compte des points suivants :
  - Si vous utilisez SCIM, l'IdP synchronise automatiquement les valeurs des attributs dans IAM Identity Center. Les attributs supplémentaires requis pour le contrôle d'accès peuvent ne pas figurer dans la liste des attributs SCIM. Dans ce cas, envisagez de collaborer avec l'administrateur informatique de votre IdP pour envoyer ces attributs à IAM Identity Center via des assertions SAML en utilisant le préfixe requis. `https://aws.amazon.com/SAML/Attributes/AccessControl:` Pour plus d'informations sur la façon de configurer les attributs utilisateur pour le contrôle d'accès dans votre IdP à envoyer via des assertions SAML, consultez le Tutoriels de mise en route
  - Si vous n'utilisez pas le SCIM, vous devez ajouter manuellement les utilisateurs et définir leurs attributs comme si vous utilisiez IAM Identity Center comme source d'identité. Accédez ensuite à la page Attributs pour le contrôle d'accès et choisissez les attributs que vous souhaitez utiliser dans les politiques.

Pour une liste complète des attributs pris en charge pour les attributs utilisateur dans IAM Identity Center et les attributs utilisateur dans votre environnement externe IdPs, consultezAttributs du fournisseur d'identité externe pris en charge.

Pour commencer à utiliser ABAC dans IAM Identity Center, consultez les rubriques suivantes.

Rubriques

Activer et configurer les attributs pour le contrôle d'accès

Pour utiliser ABAC dans tous les cas, vous devez d'abord activer ABAC à l'aide de la console IAM Identity Center ou de l'API IAM Identity Center. Si vous choisissez d'utiliser IAM Identity Center pour sélectionner des attributs, utilisez la page Attributs pour le contrôle d'accès de la console IAM Identity Center ou l'API IAM Identity Center. Si vous utilisez un fournisseur d'identité externe (IdP) comme source d'identité et que vous choisissez d'envoyer des attributs via les assertions SAML, vous configurez votre IdP pour transmettre les attributs. Si une assertion SAML transmet l'un de ces attributs, IAM Identity Center remplacera la valeur de l'attribut par la valeur du magasin d'identités IAM Identity Center. Seuls les attributs configurés dans IAM Identity Center seront envoyés pour prendre des décisions en matière de contrôle d'accès lorsque les utilisateurs se fédérent dans leurs comptes.

> **Note**
>
> Vous ne pouvez pas afficher les attributs configurés et envoyés par un IdP externe depuis la page Attributs pour le contrôle d'accès de la console IAM Identity Center. Si vous transmettez des attributs de contrôle d'accès dans les assertions SAML à partir de votre IdP externe, ces attributs sont directement envoyés au Compte AWS moment de la fédération des utilisateurs. Les attributs ne seront pas disponibles dans IAM Identity Center pour le mappage.

Activer les attributs pour le contrôle d'accès

Utilisez la procédure suivante pour activer la fonctionnalité de contrôle des attributs d'accès (ABAC) à l'aide de la console IAM Identity Center.

> **Note**
>
> Si vous disposez d'ensembles d'autorisations existants et que vous prévoyez d'activer ABAC dans votre instance IAM Identity Center, des restrictions de sécurité supplémentaires nécessitent que vous disposiez d'abord de la `iam:UpdateAssumeRolePolicy` politique.

Ces restrictions de sécurité supplémentaires ne sont pas requises si aucun ensemble d'autorisations n'a été créé dans votre compte.

Pour activer les attributs pour le contrôle d'accès

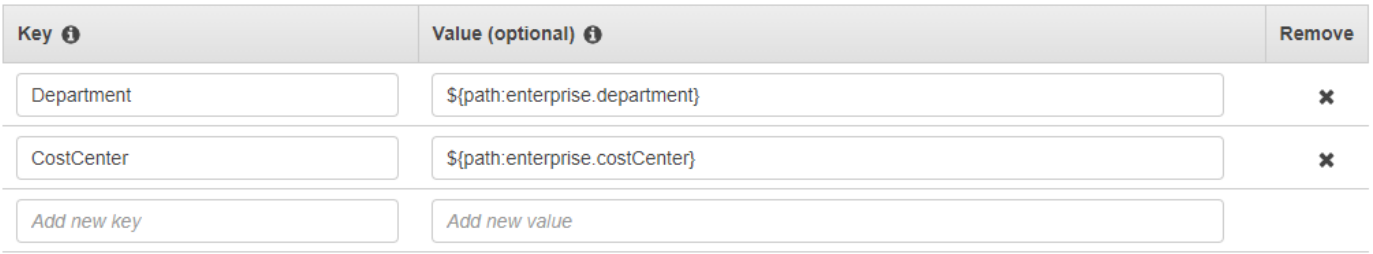
1. Ouvrez la console IAM Identity Center.
2. Choisissez les paramètres
3. Sur la page Paramètres, recherchez la zone Attributs pour les informations de contrôle d'accès, puis choisissez Activer. Passez à la procédure suivante pour le configurer.

Sélectionnez vos attributs

Utilisez la procédure suivante pour configurer les attributs de votre configuration ABAC.

Pour sélectionner vos attributs à l'aide de la console IAM Identity Center

1. Ouvrez la console IAM Identity Center.
2. Choisissez les paramètres
3. Sur la page Paramètres, choisissez l'onglet Attributs pour le contrôle d'accès, puis sélectionnez Gérer les attributs.
4. Sur la page Attributs pour le contrôle d'accès, choisissez Ajouter un attribut et entrez les détails de la clé et de la valeur. C'est ici que vous allez mapper l'attribut provenant de votre source d'identité à un attribut transmis par IAM Identity Center en tant que balise de session.



La clé représente le nom que vous donnez à l'attribut à utiliser dans les politiques. Il peut s'agir de n'importe quel nom arbitraire, mais vous devez le spécifier exactement dans les politiques que vous créez pour le contrôle d'accès. Supposons, par exemple, que vous utilisiez Okta (un IdP externe) comme source d'identité et que vous deviez transmettre les données du centre de coûts de votre organisation sous forme de balises de session. Dans Key, vous devez saisir un nom correspondant de la même manière, CostCentercomme votre nom de clé. Il est

important de noter que quel que soit le nom que vous choisissez ici, il doit également porter exactement le même nom dans votre nom `Clé de condition aws:PrincipalTag` (c'est-à-dire,`"ec2:ResourceTag/CostCenter": "${aws:PrincipalTag/CostCenter}"`).

> **Note**
>
> Utilisez un attribut à valeur unique pour votre clé, par exemple,**`Manager`**. IAM Identity Center ne prend pas en charge les attributs à valeurs multiples pour ABAC, par exemple. **`Manager, IT Systems`**

La valeur représente le contenu de l'attribut provenant de votre source d'identité configurée. Vous pouvez saisir ici n'importe quelle valeur de la table des sources d'identité appropriée répertoriée dansMappages d'attributs pour le répertoire AWS Managed Microsoft AD. Par exemple, en utilisant le contexte fourni dans l'exemple mentionné ci-dessus, vous examineriez la liste des attributs IdP pris en charge et détermineriez que la correspondance la plus proche d'un attribut pris en charge serait, **`${path:enterprise.costCenter}`**puis vous la saisiriez dans le champ Valeur. Voir la capture d'écran ci-dessus pour référence. Notez que vous ne pouvez pas utiliser de valeurs d'attributs IdP externes en dehors de cette liste pour ABAC, sauf si vous utilisez l'option de transmission d'attributs via l'assertion SAML.

5. Sélectionnez Enregistrer les modifications.

Maintenant que vous avez configuré le mappage de vos attributs de contrôle d'accès, vous devez terminer le processus de configuration ABAC. Pour ce faire, créez vos règles ABAC et ajoutez-les à vos ensembles d'autorisations et/ou à vos politiques basées sur les ressources. Cela est nécessaire pour que vous puissiez accorder aux identités des utilisateurs l'accès aux AWS ressources. Pour plus d'informations, consultez Création de politiques d'autorisation pour ABAC dans IAM Identity Center.

Désactiver des attributs pour le contrôle d'accès

Utilisez la procédure suivante pour désactiver la fonctionnalité ABAC et supprimer tous les mappages d'attributs qui ont été configurés.

Pour désactiver les attributs pour le contrôle d'accès

1. Ouvrez la console IAM Identity Center.
2. Choisissez les paramètres

3. Sur la page Paramètres, choisissez l'onglet Attributs pour le contrôle d'accès, puis sélectionnez Désactiver.
4. Dans la boîte de dialogue Désactiver les attributs pour le contrôle d'accès, passez en revue les informations et, lorsque vous êtes prêt, entrez DELETE, puis cliquez sur Confirmer.

> **Important**
>
> Cette étape supprime tous les attributs qui ont été configurés. Une fois supprimés, les attributs reçus d'une source d'identité et les attributs personnalisés que vous avez précédemment configurés ne seront pas transmis.

Création de politiques d'autorisation pour ABAC dans IAM Identity Center

Vous pouvez créer des politiques d'autorisation qui déterminent qui peut accéder à vos AWS ressources en fonction de la valeur d'attribut configurée. Lorsque vous activez ABAC et que vous spécifiez des attributs, IAM Identity Center transmet la valeur d'attribut de l'utilisateur authentifié à IAM afin de l'utiliser dans le cadre de l'évaluation des politiques.

Clé de condition aws:PrincipalTag

Vous pouvez utiliser des attributs de contrôle d'accès dans vos ensembles d'autorisations à l'aide de la clé de `aws:PrincipalTag` condition pour créer des règles de contrôle d'accès. Par exemple, dans la politique de confiance suivante, vous pouvez étiqueter toutes les ressources de votre organisation avec leurs centres de coûts respectifs. Vous pouvez également utiliser un ensemble d'autorisations unique qui accorde aux développeurs l'accès aux ressources de leur centre de coûts. Désormais, chaque fois que les développeurs se fédérent dans le compte à l'aide de l'authentification unique et de leur attribut de centre de coûts, ils n'ont accès qu'aux ressources de leurs centres de coûts respectifs. Au fur et à mesure que l'équipe ajoute des développeurs et des ressources à son projet, il vous suffit de baliser les ressources avec le centre de coûts approprié. Vous transmettez ensuite les informations du centre de coûts lors de la AWS session dans laquelle les développeurs se Comptes AWS fédérent. Ainsi, à mesure que l'organisation ajoute de nouvelles ressources et de nouveaux développeurs au centre de coûts, les développeurs peuvent gérer les ressources alignées sur leurs centres de coûts sans avoir besoin de mettre à jour les autorisations.

```
{
    "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}"
                }
            }
        }
    ]
}
```

Pour plus d'informations, consultez aws:PrincipalTaget EC2 : Démarrer ou arrêter des instances en fonction de la correspondance des balises principale et ressource dans le guide de l'utilisateur IAM.

Si les politiques contiennent des attributs non valides dans leurs conditions, la condition de politique échouera et l'accès sera refusé. Pour plus d'informations, consultez Erreur « Une erreur inattendue s'est produite » lorsqu'un utilisateur tente de se connecter à l'aide d'un fournisseur d'identité externe.

Fournisseur d'identité IAM

Lorsque vous ajoutez un accès par authentification unique à un Compte AWS, IAM Identity Center crée un fournisseur d'identité IAM dans chacun d'eux. Compte AWS Un fournisseur d'identité IAM contribue à votre Compte AWS sécurité car vous n'avez pas à distribuer ou à intégrer des informations de sécurité à long terme, telles que des clés d'accès, dans votre application.

Réparer le fournisseur d'identité IAM

Si vous supprimez ou modifiez accidentellement votre fournisseur d'identité, vous devez réappliquer manuellement vos attributions d'utilisateur et de groupe. La réapplication de vos attributions

d'utilisateur et de groupe permet de recréer le fournisseur d'identité. Pour plus d'informations, consultez :

- Gérez l'accès à Comptes AWS
- Gérez l'accès aux applications

Rôles liés à un service

Les rôles liés à un service sont des autorisations IAM prédéfinies qui permettent à IAM Identity Center de déléguer et d'appliquer les utilisateurs disposant d'un accès par authentification unique à des utilisateurs spécifiques Comptes AWS de votre organisation dans. AWS Organizations Le service active cette fonctionnalité en attribuant un rôle lié au service Compte AWS dans chaque élément de son organisation. Le service permet ensuite à d'autres AWS services tels que IAM Identity Center de tirer parti de ces rôles pour effectuer des tâches liées au service. Pour plus d'informations, consultez la section AWS Organizations et les rôles liés à un service.

Lorsque vous activez IAM Identity Center, IAM Identity Center crée un rôle lié à un service dans tous les comptes de l'organisation dans. AWS Organizations IAM Identity Center crée également le même rôle lié au service dans chaque compte ajouté ultérieurement à votre organisation. Ce rôle permet à IAM Identity Center d'accéder aux ressources de chaque compte en votre nom. Pour plus d'informations, consultez Gérez l'accès à Comptes AWS.

Les rôles liés à un service créés dans chacun d'eux Compte AWS sont nommés. `AWSServiceRoleForSSO` Pour plus d'informations, voir Utilisation de rôles liés à un service pour IAM Identity Center.

Gérez l'accès aux applications

Vous pouvez ainsi contrôler les personnes autorisées à accéder à vos applications par authentification unique. AWS IAM Identity Center Les utilisateurs peuvent accéder facilement à ces applications une fois qu'ils ont utilisé les informations d'identification de leur annuaire pour se connecter.

IAM Identity Center communique en toute sécurité avec ces applications grâce à une relation de confiance entre IAM Identity Center et le fournisseur de services de l'application. Cette confiance peut être créée de différentes manières, selon le type d'application.

IAM Identity Center prend en charge deux types d'applications : les applications AWS gérées et les applications gérées par le client. AWS les applications gérées sont configurées directement depuis les consoles d'application pertinentes ou via les API de l'application. Les applications gérées par le client doivent être ajoutées à la console IAM Identity Center et configurées avec les métadonnées appropriées à la fois pour IAM Identity Center et pour le fournisseur de services.

Après avoir configuré les applications pour qu'elles fonctionnent avec IAM Identity Center, vous pouvez gérer les utilisateurs ou les groupes qui accèdent aux applications. Par défaut, aucun utilisateur n'est affecté aux applications.

Vous pouvez également accorder à vos employés l'accès AWS Management Console au formulaire spécifique Compte AWS de votre organisation. Pour plus d'informations, consultez Gérez l'accès à Comptes AWS.

Rubriques

AWS applications gérées

AWS les applications gérées s'intègrent à IAM Identity Center et peuvent l'utiliser pour l'authentification et les services d'annuaire.

L'intégration des applications AWS gérées à IAM Identity Center vous permet d'attribuer plus facilement l'accès aux utilisateurs, sans qu'il soit nécessaire de configurer une fédération ou une synchronisation des utilisateurs et des groupes distinctes pour chaque application. Vous pouvez connecter la source d'identité que vous souhaitez utiliser pour l'authentification une seule fois, et vous bénéficiez d'une vue unique des attributions des utilisateurs et des groupes. Les administrateurs des applications qui permettent une propagation fiable des identités peuvent définir et auditer l'accès aux ressources de leurs applications en fonction de l'appartenance d'un utilisateur ou d'un groupe d'utilisateurs, sans avoir à les associer à des rôles IAM.

AWS les applications gérées fournissent une interface utilisateur administrative que vous pouvez utiliser pour gérer l'accès aux ressources de l'application. Par exemple, QuickSight les administrateurs peuvent assigner aux utilisateurs l'accès aux tableaux de bord en fonction de leur appartenance à un groupe. La plupart des applications AWS gérées offrent également une AWS Management Console expérience qui vous permet d'attribuer des utilisateurs à l'application. L'expérience de console de ces applications peut intégrer les deux fonctions, afin de combiner les capacités d'attribution des utilisateurs avec la capacité de gérer l'accès aux ressources de l'application.

AWS les applications gérées intégrées à IAM Identity Center incluent :

AWS applications gérées qui s'intègrent à IAM Identity Center

AWS application gérée	Intégré à l'instance organisationnelle d'IAM Identity Center	Intégré aux instances de compte d'IAM Identity Center	Permet une propagation d'identité fiable via IAM Identity Center
Amazon Athena SQL	 O	 O	 Oui

AWS application gérée	Intégré à l'instance organisationnelle d'IAM Identity Center	Intégré aux instances de compte d'IAM Identity Center	Permet une propagation d'identité fiable via IAM Identity Center
Amazon CodeCatalyst	 O	 O	 Non
Carnets Amazon EMR	 O	 N	 Non
Amazon EMR sur Amazon EC2	 O	 O	 Oui
Amazon EMR Studio	 O	 O	 Oui
Amazon Kendra	 O	 N	 Non
Amazon Managed Grafana	 O	 N	 Non
Amazon Monitron	 O	 N	 Non
Amazon Nimble Studio	 O	 N	 Non

AWS application gérée	Intégré à [l'instance organisationnelle d'IAM Identity Center]	Intégré aux [instances de compte d'IAM Identity Center]	Permet une [propagation d'identité fiable] via IAM Identity Center
Amazon Pinpoint	 O	 N	 Non
Amazon Q Business	 O	 O	 Non
Développeur Amazon Q	 O	 O *	 Non
Amazon QuickSight	 O	 O	 Oui
Amazon Redshift	 O	 O	 Oui
Subventions d'accès Amazon S3	 O	 O	 Oui
Amazon SageMaker Studio	 O	 N	 Non

AWS application gérée	Intégré à l'instance organisationnelle d'IAM Identity Center	Intégré aux instances de compte d'IAM Identity Center	Permet une propagation d'identité fiable via IAM Identity Center
WorkSpaces Site Web d'Amazon	 O	 N	 Non
AWS CLI	 O	 N	 Non
AWS Deadline Cloud	 O	 O	 Non
AWS IoT Events	 O	 N	 Non
AWS IoT Fleet Hub	 O	 N	 Non
AWS IoT SiteWise	 O	 N	 Non
AWS Lake Formation	 O	 O	 Oui
AWS Supply Chain	 O	 N	 Non

AWS application gérée	Intégré à l'instance organisationnelle d'IAM Identity Center	Intégré aux instances de compte d'IAM Identity Center	Permet une propagation d'identité fiable via IAM Identity Center
AWS Systems Manager	 O	 N	 Non
Accès vérifié par AWS	 O	 N	 Non

* Les instances de compte d'IAM Identity Center sont prises en charge, sauf si vos utilisateurs ont besoin d'accéder à Amazon Q dans la AWS console.

Rubriques

- Contrôle de l'accès
- Coordination des tâches administratives
- Configuration d'IAM Identity Center pour partager les informations d'identité
- Considérations relatives au partage des informations d'identité dans Comptes AWS
- Activation de sessions de console basées sur l'identité
- Limiter l'utilisation des applications AWS gérées
- Afficher les détails d'une application AWS gérée
- Désactivation d'une application AWS gérée

Contrôle de l'accès

L'accès aux applications AWS gérées est contrôlé de deux manières :

- Entrée initiale dans l'application : IAM Identity Center gère cela par le biais d'assignations à l'application. Par défaut, les affectations sont obligatoires pour les applications AWS gérées.

- Accès aux ressources de l'application : l'application gère cela par le biais d'affectations de ressources indépendantes qu'elle contrôle.

Coordination des tâches administratives

Si vous êtes administrateur d'applications, vous pouvez choisir d'exiger ou non des affectations à une application. Si des attributions sont requises, lorsque les utilisateurs se connectent au portail AWS d'accès, seuls les utilisateurs affectés à l'application directement ou par le biais d'une attribution de groupe peuvent voir la vignette de l'application. Si aucune attribution n'est requise, vous pouvez également autoriser tous les utilisateurs d'IAM Identity Center à accéder à l'application. Dans ce cas, l'application gère l'accès aux ressources et la vignette de l'application est visible par tous les utilisateurs qui visitent le portail AWS d'accès.

Si vous êtes administrateur d'IAM Identity Center, vous pouvez utiliser la console IAM Identity Center pour supprimer des assignations aux applications AWS gérées. Avant de supprimer des attributions, nous vous recommandons de vous concerter avec l'administrateur de l'application. Vous devez également vous coordonner avec l'administrateur de l'application si vous envisagez de modifier le paramètre qui détermine si des affectations sont requises ou d'automatiser les affectations d'applications.

Configuration d'IAM Identity Center pour partager les informations d'identité

IAM Identity Center fournit une banque d'identités qui contient les attributs des utilisateurs et des groupes, à l'exception des informations de connexion. Vous pouvez utiliser l'une des méthodes suivantes pour maintenir à jour les utilisateurs et les groupes de votre banque d'identités IAM Identity Center :

- Utilisez le magasin d'identités IAM Identity Center comme source d'identité principale. Si vous choisissez cette méthode, vous gérez vos utilisateurs, leurs identifiants de connexion et les groupes depuis la console IAM Identity Center ou AWS Command Line Interface ()AWS CLI. Pour plus d'informations, consultez Gestion des identités dans IAM Identity Center.
- Configurez le provisionnement (synchronisation) des utilisateurs et des groupes provenant de l'une des sources d'identité suivantes vers votre banque d'identités IAM Identity Center :
  - Active Directory — Pour plus d'informations, consultezSe connecter à un Microsoft AD annuaire.
  - Fournisseur d'identité externe : pour plus d'informations, consultezConnectez-vous à un fournisseur d'identité externe.

Si vous choisissez cette méthode de provisionnement, vous continuez à gérer vos utilisateurs et vos groupes depuis votre source d'identité, et ces modifications sont synchronisées avec le magasin d'identités IAM Identity Center.

Quelle que soit la source d'identité que vous choisissez, IAM Identity Center peut partager les informations relatives aux utilisateurs et aux groupes avec les applications AWS gérées. Ainsi, vous pouvez connecter une source d'identité à IAM Identity Center une seule fois, puis partager les informations d'identité avec plusieurs applications du AWS Cloud. Il n'est donc plus nécessaire de configurer indépendamment la fédération et le provisionnement des identités pour chaque application. Cette fonctionnalité de partage permet également de donner facilement à vos utilisateurs l'accès à de nombreuses applications de différentes manières Comptes AWS.

Considérations relatives au partage des informations d'identité dans Comptes AWS

IAM Identity Center prend en charge les attributs les plus couramment utilisés dans toutes les applications. Ces attributs incluent le prénom et le nom de famille, le numéro de téléphone, l'adresse e-mail, l'adresse et la langue préférée. Examinez attentivement quelles applications et quels comptes peuvent utiliser ces informations personnelles identifiables.

Vous pouvez contrôler l'accès à ces informations de l'une des manières suivantes. Vous pouvez choisir d'activer l'accès uniquement dans le compte AWS Organizations de gestion ou dans tous les comptes de AWS Organizations. Vous pouvez également utiliser des politiques de contrôle des services (SCP) pour contrôler quelles applications peuvent accéder aux informations dans quels comptes. AWS Organizations Par exemple, si vous activez l'accès uniquement dans le compte de AWS Organizations gestion, les applications des comptes membres n'ont pas accès aux informations. Toutefois, si vous activez l'accès dans tous les comptes, vous pouvez utiliser les SCP pour interdire l'accès à toutes les applications, à l'exception de celles que vous souhaitez autoriser.

Activation de sessions de console basées sur l'identité

Une session basée sur l'identité pour la console améliore la session de AWS console d'un utilisateur en fournissant un contexte utilisateur supplémentaire pour personnaliser l'expérience de cet utilisateur. Cette fonctionnalité est actuellement prise en charge pour les utilisateurs d'Amazon Q dans la AWS console.

Vous pouvez activer les sessions de console basées sur l'identité sans modifier les modèles d'accès existants ou la fédération dans la AWS console aujourd'hui. Si vos utilisateurs se connectent à la AWS console via IAM (par exemple, s'ils se connectent en tant qu'utilisateurs IAM ou via un accès fédéré avec IAM), ils peuvent continuer à utiliser ces méthodes. Si vos utilisateurs se connectent au portail AWS d'accès, ils peuvent continuer à utiliser leurs informations d'identification utilisateur IAM Identity Center.

Rubriques

Prérequis et considérations

Avant d'activer les sessions de console basées sur l'identité, passez en revue les conditions préalables et les considérations suivantes :

- Vous devez activer les sessions de console basées sur l'identité pour les utilisateurs qui ont besoin d'accéder à Amazon Q dans la AWS console.
- Les sessions de console basées sur l'identité ne sont actuellement prises en charge que pour une utilisation avec Amazon Q dans la AWS console.
- Les sessions de console basées sur l'identité nécessitent une instance organisationnelle d'IAM Identity Center.
- L'intégration à Amazon Q n'est pas prise en charge si vous activez IAM Identity Center dans le cadre d'un Région AWS opt-in.
- Une fois que vous avez activé les sessions de console basées sur l'identité, vous ne pouvez pas désactiver cette fonctionnalité.
- Pour activer les sessions de console basées sur l'identité, vous devez disposer des autorisations suivantes :
  - `sso:CreateApplication`
  - `sso:GetSharedSsoConfiguration`
  - `sso:ListApplications`
  - `sso:PutApplicationAssignmentConfiguration`
  - `sso:PutApplicationAuthenticationMethod`

- `sso:PutApplicationGrant`
- `sso:PutApplicationAccessScope`
- `signin:CreateTrustedIdentityPropagationApplicationForConsole`
- `signin:ListTrustedIdentityPropagationApplicationForConsole`
-

- Pour permettre à vos utilisateurs d'utiliser des sessions de console basées sur l'identité, vous devez leur accorder l'`sts:setContext`autorisation dans le cadre d'une politique basée sur l'identité. Pour plus d'informations, consultez la section Autorisation des utilisateurs à utiliser des sessions de console basées sur l'identité.

Comment activer les identity-aware-console sessions

Vous pouvez activer les sessions de console sensibles à l'identité dans la console Amazon Q ou dans la console IAM Identity Center.

Activez les sessions de console basées sur l'identité dans la console Amazon Q

Avant d'activer les sessions de console basées sur l'identité, vous devez disposer d'une instance d'organisation d'IAM Identity Center connectée à une source d'identité. Si vous avez déjà configuré IAM Identity Center, passez à l'étape 3.

1. Ouvrez la console IAM Identity Center. Choisissez Activer et créez une instance d'organisation d'IAM Identity Center. Pour plus d'informations, veuillez consulter Activant AWS IAM Identity Center.
2. Connectez votre source d'identité à IAM Identity Center et connectez les utilisateurs à IAM Identity Center. Vous pouvez choisir le répertoire IAM Identity Center par défaut comme source d'identité, ou vous pouvez utiliser un autre fournisseur d'identité. Pour plus d'informations, consultez Tutoriels de mise en route.
3. Une fois que vous avez terminé de configurer IAM Identity Center, ouvrez la console Amazon Q et suivez les étapes décrites dans la section Abonnements du manuel Amazon Q Developer User Guide. Assurez-vous d'activer les sessions de console basées sur l'identité.

> **Note**
>
> Si vous ne disposez pas des autorisations suffisantes pour activer les sessions de console basées sur l'identité, vous devrez peut-être demander à un administrateur IAM

Identity Center d'effectuer cette tâche pour vous dans la console IAM Identity Center. Pour en savoir plus, consultez la procédure suivante.

Activer les sessions de console basées sur l'identité dans la console IAM Identity Center

Si vous êtes administrateur d'IAM Identity Center, un autre administrateur peut vous demander d'activer les sessions de console basées sur l'identité dans la console IAM Identity Center.

1. Ouvrez la console IAM Identity Center.
2. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
3. Sous Activer les sessions basées sur l'identité, sélectionnez Activer.
4. Dans le deuxième message, sélectionnez Activer.
5. Une fois que vous avez terminé d'activer les sessions de console basées sur l'identité, un message de confirmation apparaît en haut de la page Paramètres.
6. Dans la section Détails, le statut des sessions basées sur l'identité est Activé.

Comment fonctionnent les sessions de console basées sur l'identité

Avec les sessions de console basées sur l'identité, les utilisateurs d'Amazon Q peuvent se connecter AWS, ouvrir le site Web AWS Management Console ou un autre AWS site Web, choisir l'icône Amazon Q, démarrer une discussion ou utiliser d'autres fonctionnalités prises en charge. AWS Pour plus d'informations, consultez le guide de l'utilisateur Amazon Q Developer.

IAM Identity Center améliore la session de console actuelle d'un utilisateur pour inclure l'ID utilisateur IAM Identity Center actif et l'ID de session IAM Identity Center.

Les sessions de console basées sur l'identité incluent les trois valeurs suivantes :

- ID utilisateur du magasin d'identités (boutique d'identité : UserId) : cette valeur est utilisée pour identifier de manière unique un utilisateur dans la source d'identité connectée à IAM Identity Center.
- ARN du répertoire du magasin d'identités (boutique d'identité : IdentityStoreArn) : cette valeur est l'ARN du magasin d'identités connecté à IAM Identity Center et dans lequel vous pouvez rechercher des attributs. `identitystore:UserId`
- ID de session IAM Identity Center : cette valeur indique si la session IAM Identity Center de l'utilisateur est toujours valide.

Les valeurs sont les mêmes, mais obtenues de différentes manières et ajoutées à différents moments du processus, en fonction de la manière dont l'utilisateur se connecte :

- IAM Identity Center (portail AWS d'accès) : dans ce cas, l'ID utilisateur et les valeurs ARN du magasin d'identités de l'utilisateur sont déjà fournis dans la session IAM Identity Center active. IAM Identity Center améliore la session en cours en ajoutant uniquement l'ID de session.
- Autres méthodes de connexion : si l'utilisateur se connecte en AWS tant qu'utilisateur IAM, avec un rôle IAM ou en tant qu'utilisateur fédéré avec IAM, aucune de ces valeurs n'est fournie. IAM Identity Center améliore la session en cours en ajoutant l'ID utilisateur de la banque d'identités, l'ARN du répertoire de la banque d'identités et l'ID de session.

Limiter l'utilisation des applications AWS gérées

Lorsque vous activez IAM Identity Center pour la première fois, il AWS autorise l'utilisation automatique des applications AWS gérées dans tous les comptes de. AWS Organizations Pour contraindre les applications, vous devez implémenter des SCP. Vous pouvez utiliser les SCP pour bloquer l'accès aux informations des utilisateurs et des groupes IAM Identity Center et pour empêcher le démarrage de l'application, sauf pour les comptes désignés.

Afficher les détails d'une application AWS gérée

Une fois que vous avez connecté une application AWS gérée à IAM Identity Center à l'aide de la console ou des API de l'application, celle-ci est enregistrée auprès d'IAM Identity Center. Une fois qu'une application est enregistrée auprès d'IAM Identity Center, vous pouvez consulter des informations détaillées sur l'application dans la console IAM Identity Center.

Pour afficher les informations relatives à une application AWS gérée dans la console IAM Identity Center

1. Ouvrez la console IAM Identity Center.
2. Choisissez Applications.
3. Choisissez l'onglet Applications AWS gérées.
4. Dans la liste des applications, choisissez le nom de l'application pour laquelle vous souhaitez afficher des informations détaillées.
5. Les informations relatives à l'application indiquent si des affectations d'utilisateurs et de groupes sont requises et, le cas échéant, des utilisateurs et des groupes assignés et des applications

fiables pour la propagation des identités. Pour plus d'informations sur la propagation d'identités fiables, consultezPropagation d'identité approuvée entre applications.

Désactivation d'une application AWS gérée

Pour empêcher les utilisateurs de s'authentifier auprès d'une application AWS gérée, vous pouvez désactiver l'application dans la console IAM Identity Center.

> **Warning**
>
> La désactivation d'une application supprime toutes les autorisations utilisateur associées à cette application, déconnecte l'application d'IAM Identity Center et la rend inaccessible. Si vous êtes administrateur d'IAM Identity Center, nous vous recommandons de vous coordonner avec l'administrateur de l'application avant d'effectuer cette tâche.

Pour désactiver une application AWS gérée

1. Ouvrez la console IAM Identity Center.
2. Choisissez Applications.
3. Sur la page Applications, sous Applications AWS gérées, choisissez l'application que vous souhaitez désactiver.
4. Une fois l'application sélectionnée, choisissez Actions, puis sélectionnez Désactiver.
5. Dans la boîte de dialogue Suspendre l'application, choisissez Suspendre.
6. Dans la liste des applications AWS gérées, le statut de l'application apparaît comme Inactif.

Applications gérées par le client

Avec IAM Identity Center, vous pouvez créer ou connecter des utilisateurs du personnel et gérer de manière centralisée leur accès à toutes leurs Comptes AWS applications. IAM Identity Center agit comme un service d'identité central et propose différentes méthodes d'authentification à vos utilisateurs. Si vous utilisez déjà un fournisseur d'identité (IdP), IAM Identity Center peut s'intégrer à votre IdP afin que vous puissiez configurer vos utilisateurs et vos groupes dans IAM Identity Center et utiliser votre IdP pour l'authentification.

Si vous utilisez des applications gérées par le client qui prennent en charge le protocole SAML 2.0, vous pouvez fédérer votre IdP à IAM Identity Center via SAML 2.0 et utiliser IAM Identity Center pour gérer l'accès des utilisateurs à ces applications. IAM Identity Center fournit un catalogue d'applications couramment utilisées qui prennent en charge le protocole SAML 2.0, telles que Salesforce et Microsoft 365. Ce catalogue est disponible dans la console IAM Identity Center. Vous pouvez également configurer vos propres applications SAML 2.0.

> **Note**
>
> Si vous avez des applications gérées par le client qui prennent en charge OAuth 2.0 et que vos utilisateurs ont besoin d'accéder à des AWS services depuis ces applications, vous pouvez utiliser la propagation d'identité sécurisée. Grâce à la propagation d'identité sécurisée, un utilisateur peut se connecter à une application, et cette application peut transmettre l'identité de l'utilisateur dans les demandes d'accès aux données AWS des services. Pour plus d'informations, consultez Utilisation d'une propagation d'identité fiable avec des applications gérées par le client.

Rubriques

SAML 2.0 et OAuth 2.0

IAM Identity Center vous permet de fournir à vos utilisateurs un accès par authentification unique aux applications SAML 2.0 ou OAuth 2.0. Les rubriques suivantes fournissent une présentation générale de SAML 2.0 et OAuth 2.0.

Rubriques

SAML 2.0

SAML 2.0 est une norme industrielle utilisée pour échanger en toute sécurité des assertions SAML qui transmettent des informations sur un utilisateur entre une autorité SAML (appelée fournisseur

d'identité ou IdP) et un consommateur SAML 2.0 (appelé fournisseur de services ou SP). IAM Identity Center utilise ces informations pour fournir un accès d'authentification unique fédéré aux utilisateurs autorisés à utiliser les applications du AWS portail d'accès.

OAuth 2.0

OAuth 2.0 est un protocole qui permet aux applications d'accéder aux données des utilisateurs et de les partager en toute sécurité sans partager de mots de passe. Cette fonctionnalité fournit aux utilisateurs un moyen sécurisé et standardisé d'autoriser les applications à accéder à leurs ressources. L'accès est facilité par différents flux de subventions OAuth 2.0.

IAM Identity Center permet aux applications qui s'exécutent sur des clients publics de récupérer des informations d'identification temporaires pour accéder Comptes AWS et fournir des services par programmation au nom de leurs utilisateurs. Les clients publics sont généralement des ordinateurs de bureau, des ordinateurs portables ou d'autres appareils mobiles utilisés pour exécuter des applications localement. Les exemples d' AWS applications qui s'exécutent sur des clients publics incluent le AWS Command Line Interface (AWS CLI) et les kits de développement AWS logiciel (SDK). AWS Toolkit Pour permettre à ces applications d'obtenir des informations d'identification, IAM Identity Center prend en charge certaines parties des flux OAuth 2.0 suivants :

- Octroi de code d'autorisation avec clé de preuve pour l'échange de code (PKCE) (RFC 6749 et RFC 7636)
- Octroi d'autorisation d'appareil (RFC 8628)

> **Note**
>
> Ces types de subventions ne peuvent être utilisés Services AWS que s'ils prennent en charge cette fonctionnalité. Il est possible que ces services ne prennent pas en charge ce type de subvention du tout Régions AWS. Reportez-vous à la documentation pertinente Services AWS pour les différences régionales.

OpenID Connect (OIDC) est un protocole d'authentification basé sur le framework OAuth 2.0. L'OIDC indique comment utiliser OAuth 2.0 pour l'authentification. Par le biais des API du service IAM Identity Center OIDC, une application enregistre un client OAuth 2.0 et utilise l'un de ces flux pour obtenir un jeton d'accès qui fournit des autorisations aux API protégées par IAM Identity Center. Une application définit les étendues d'accès pour déclarer l'utilisateur d'API auquel elle est destinée. Une fois que

vous, en tant qu'administrateur du centre d'identité IAM, avez configuré votre source d'identité, les utilisateurs finaux de votre application doivent terminer un processus de connexion, s'ils ne l'ont pas déjà fait. Vos utilisateurs finaux doivent ensuite donner leur accord pour autoriser l'application à effectuer des appels d'API. Ces appels d'API sont effectués à l'aide des autorisations des utilisateurs. En réponse, IAM Identity Center renvoie un jeton d'accès à l'application contenant les étendues d'accès auxquelles les utilisateurs ont consenti.

Utilisation d'un flux de subventions OAuth 2.0

Les flux de subventions OAuth 2.0 ne sont disponibles que via les applications AWS gérées qui les prennent en charge. Pour utiliser un flux OAuth 2.0, votre instance d'IAM Identity Center et toutes les applications AWS gérées prises en charge que vous utilisez doivent être déployées en une seule fois. Région AWS Reportez-vous à la documentation de chacune Service AWS pour déterminer la disponibilité régionale des applications AWS gérées et l'instance d'IAM Identity Center que vous souhaitez utiliser.

Pour utiliser une application qui utilise un flux OAuth 2.0, l'utilisateur final doit saisir l'URL à laquelle l'application se connectera et s'enregistrera auprès de votre instance d'IAM Identity Center. Selon l'application, en tant qu'administrateur, vous devez fournir à vos utilisateurs l'URL du portail AWS d'accès ou l'URL de l'émetteur de votre instance d'IAM Identity Center. Vous trouverez ces deux paramètres sur la page des paramètres de la console IAM Identity Center. Pour plus d'informations sur la configuration d'une application cliente, reportez-vous à la documentation de cette application.

L'expérience de l'utilisateur final en matière de connexion à une application et de fourniture de son consentement varie selon que l'application utilise le Octroi de code d'autorisation avec PKCE ouOctroi d'autorisation d'appareil.

Octroi de code d'autorisation avec PKCE

Ce flux est utilisé par les applications qui s'exécutent sur un appareil doté d'un navigateur.

1. Une fenêtre de navigateur s'ouvre.
2. Si l'utilisateur ne s'est pas authentifié, le navigateur le redirige pour terminer l'authentification utilisateur.
3. Après authentification, l'utilisateur s'affiche sur un écran de consentement qui affiche les informations suivantes :
   - Le nom de l'application
   - Les étendues d'accès que l'application demande le consentement pour utiliser

4. L'utilisateur peut annuler le processus de consentement ou donner son consentement et l'application procède à l'accès en fonction des autorisations de l'utilisateur.

Octroi d'autorisation d'appareil

Ce flux peut être utilisé par les applications qui s'exécutent sur un appareil avec ou sans navigateur. Lorsque l'application lance le flux, elle présente une URL et un code utilisateur que l'utilisateur doit vérifier ultérieurement dans le flux. Le code utilisateur est nécessaire car l'application qui initie le flux est peut-être exécutée sur un appareil différent de celui sur lequel l'utilisateur donne son consentement. Le code garantit que l'utilisateur consent au flux qu'il a initié sur l'autre appareil.

1. Lorsque le flux est lancé à partir d'un appareil doté d'un navigateur, une fenêtre de navigateur s'ouvre. Lorsque le flux est lancé à partir d'un appareil sans navigateur, l'utilisateur doit ouvrir un navigateur sur un autre appareil et accéder à l'URL présentée par l'application.
2. Dans les deux cas, si l'utilisateur ne s'est pas authentifié, le navigateur le redirige pour terminer l'authentification de l'utilisateur.
3. Après authentification, l'utilisateur s'affiche sur un écran de consentement qui affiche les informations suivantes :
   - Le nom de l'application
   - Les étendues d'accès que l'application demande le consentement pour utiliser
   - Le code utilisateur que l'application a présenté à l'utilisateur
4. L'utilisateur peut annuler le processus de consentement ou donner son consentement et l'application procède à l'accès en fonction des autorisations de l'utilisateur.

Étendue d'accès

Une étendue définit l'accès à un service pour un service accessible via un flux OAuth 2.0. Les étendues permettent au service, également appelé serveur de ressources, de regrouper les autorisations liées aux actions et aux ressources du service, et elles spécifient les opérations grossières que les clients OAuth 2.0 peuvent demander. Lorsqu'un client OAuth 2.0 s'enregistre auprès du service IAM Identity Center OIDC, le client spécifie les étendues dans lesquelles il déclare les actions prévues, pour lesquelles l'utilisateur doit donner son consentement.

Les clients OAuth 2.0 utilisent `scope` les valeurs définies dans la section 3.3 d'OAuth 2.0 (RFC 6749) pour spécifier les autorisations demandées pour un jeton d'accès. Les clients peuvent spécifier un maximum de 25 étendues lorsqu'ils demandent un jeton d'accès. Lorsqu'un utilisateur donne son

consentement lors d'une attribution de code d'autorisation avec PKCE ou Device Authorization Grant flow, IAM Identity Center encode les étendues dans le jeton d'accès qu'il renvoie.

AWS ajoute des champs d'application à IAM Identity Center pour qu'ils soient pris en charge. Services AWS Le tableau suivant répertorie les étendues prises en charge par le service IAM Identity Center OIDC lorsque vous enregistrez un client public.

Étendue d'accès prise en charge par le service IAM Identity Center OIDC lors de l'enregistrement d'un client public

Portée	Description	Services pris en charge par
`sso:account:access`	Accédez aux comptes gérés par IAM Identity Center et aux ensembles d'autorisations.	IAM Identity Center
`codewhisperer:analysis`	Activez l'accès à l'analyse du code Amazon Q Developer.	ID de constructeur AWS et IAM Identity Center
`codewhisperer:completions`	Activez l'accès aux suggestions de code en ligne d'Amazon Q.	ID de constructeur AWS et IAM Identity Center
`codewhisperer:conversations`	Activez l'accès au chat Amazon Q.	ID de constructeur AWS et IAM Identity Center
`codewhisperer:taskassist`	Activez l'accès à Amazon Q Developer Agent pour le développement de logiciels.	ID de constructeur AWS et IAM Identity Center
`codewhisperer:transformations`	Activez l'accès à Amazon Q Developer Agent pour la transformation du code.	ID de constructeur AWS et IAM Identity Center
`codecatalyst:read_write`	Lisez et écrivez sur vos CodeCatalyst ressources Amazon pour accéder à toutes vos ressources existantes.	ID de constructeur AWS et IAM Identity Center

Configuration d'applications SAML 2.0 gérées par le client

Si vous utilisez des applications gérées par le client qui prennent en charge le protocole SAML 2.0, vous pouvez fédérer votre IdP à IAM Identity Center via SAML 2.0 et utiliser IAM Identity Center pour gérer l'accès des utilisateurs à ces applications. Vous pouvez sélectionner une application SAML 2.0 dans un catalogue d'applications couramment utilisées dans la console IAM Identity Center, ou vous pouvez configurer votre propre application SAML 2.0.

> **Note**
>
> Si vous avez des applications gérées par le client qui prennent en charge OAuth 2.0 et que vos utilisateurs ont besoin d'accéder à des AWS services depuis ces applications, vous pouvez utiliser la propagation d'identité sécurisée. Grâce à la propagation d'identité sécurisée, un utilisateur peut se connecter à une application, et cette application peut transmettre l'identité de l'utilisateur dans les demandes d'accès aux données AWS des services. Pour plus d'informations, consultez Utilisation d'une propagation d'identité fiable avec des applications gérées par le client.

Rubriques

- Catalogue d'applications IAM Identity Center
- Configurez votre propre application SAML 2.0

Catalogue d'applications IAM Identity Center

Vous pouvez utiliser le catalogue d'applications de la console IAM Identity Center pour ajouter de nombreuses applications SAML 2.0 couramment utilisées qui fonctionnent avec IAM Identity Center. Les exemples incluent Salesforce, Box et Microsoft 365.

La plupart des applications fournissent des informations détaillées sur la façon de configurer la confiance entre IAM Identity Center et le fournisseur de services de l'application. Ces informations sont disponibles sur la page de configuration de l'application, une fois que vous l'avez sélectionnée dans le catalogue. Après avoir configuré l'application, vous pouvez attribuer l'accès à des utilisateurs ou à des groupes dans IAM Identity Center selon vos besoins.

Rubriques

- Configuration d'une application à partir du catalogue d'applications

Configuration d'une application à partir du catalogue d'applications

Utilisez cette procédure pour configurer une relation de confiance SAML 2.0 entre IAM Identity Center et le fournisseur de services de votre application.

Avant de commencer cette procédure, il est utile de disposer du fichier d'échange de métadonnées du fournisseur de services afin de configurer plus efficacement la confiance. Si vous n'avez pas ce fichier, vous pouvez toujours utiliser cette procédure pour le configurer manuellement.

Pour ajouter et configurer une application depuis le catalogue d'applications

1. Ouvrez la console IAM Identity Center.
2. Choisissez Applications.
3. Choisissez l'onglet Géré par le client.
4. Choisissez Add application (Ajouter une application).
5. Sur la page Sélectionner le type d'application, sous Préférences de configuration, choisissez Je souhaite sélectionner une application dans le catalogue.
6. Sous Catalogue d'applications, commencez à taper le nom de l'application que vous souhaitez ajouter dans le champ de recherche.
7. Choisissez le nom de l'application dans la liste lorsqu'elle apparaît dans les résultats de recherche, puis cliquez sur Suivant.
8. Sur la page Configurer l'application, les champs Nom d'affichage et Description sont préremplis avec les informations pertinentes pour l'application. Vous pouvez modifier ces informations.
9. Sous les métadonnées du IAM Identity Center, procédez comme suit :

    a. Dans le fichier de métadonnées SAML d'IAM Identity Center, choisissez Télécharger pour télécharger les métadonnées du fournisseur d'identité.

    b. Sous le certificat IAM Identity Center, choisissez Télécharger le certificat pour télécharger le certificat du fournisseur d'identité.

> **Note**
>
> Vous aurez besoin de ces fichiers ultérieurement lorsque vous configurerez l'application à partir du site Web du fournisseur de services. Suivez les instructions de ce fournisseur.

10. (Facultatif) Sous Propriétés de l'application, vous pouvez spécifier l'URL de démarrage de l'application, l'état du relais et la durée de la session. Pour plus d'informations, consultez Configuration des propriétés de l'application dans la console IAM Identity Center.
11. Sous Métadonnées de l'application, effectuez l'une des opérations suivantes :

    a. Si vous avez un fichier de métadonnées, choisissez Télécharger le fichier de métadonnées SAML de l'application. Sélectionnez ensuite Choisir un fichier pour rechercher et sélectionner le fichier de métadonnées.

    b. Si vous n'avez pas de fichier de métadonnées, choisissez Tapez manuellement vos valeurs de métadonnées, puis fournissez l'URL de l'application ACS et les valeurs d'audience SAML de l'application.
12. Sélectionnez Envoyer. Vous êtes redirigé vers la page de détails de l'application que vous venez d'ajouter.

Configurez votre propre application SAML 2.0

Vous pouvez configurer vos propres applications qui autorisent la fédération d'identités à l'aide de SAML 2.0 et les ajouter à IAM Identity Center. La plupart des étapes de configuration de vos propres applications SAML 2.0 sont identiques à celles de configuration d'une application SAML 2.0 à partir du catalogue d'applications de la console IAM Identity Center. Toutefois, vous devez également fournir des mappages d'attributs SAML supplémentaires pour vos propres applications SAML 2.0. Ces mappages permettent à IAM Identity Center de remplir correctement l'assertion SAML 2.0 pour votre application. Vous pouvez fournir ce mappage d'attributs SAML supplémentaire lorsque vous configurez l'application pour la première fois. Vous pouvez également fournir des mappages d'attributs SAML 2.0 sur la page de détails de l'application dans la console IAM Identity Center.

Utilisez la procédure suivante pour configurer une relation de confiance SAML 2.0 entre IAM Identity Center et le fournisseur de services de votre application SAML 2.0. Avant de commencer cette procédure, vérifiez que vous avez le certificat et les fichiers d'échange de métadonnées du fournisseur de services afin de finaliser la configuration de l'approbation.

Pour configurer votre propre application SAML 2.0

1. Ouvrez la console IAM Identity Center.
2. Choisissez Applications.
3. Choisissez l'onglet Géré par le client.
4. Choisissez Add application (Ajouter une application).

5. Sur la page Sélectionner le type d'application, sous Préférences de configuration, choisissez J'ai une application que je souhaite configurer.
6. Sous Type d'application, choisissez SAML 2.0.
7. Choisissez Suivant.
8. Sur la page Configurer l'application, sous Configurer l'application, entrez un nom d'affichage pour l'application, tel que**`MyApp`**. Entrez ensuite une description.
9. Sous les métadonnées du IAM Identity Center, procédez comme suit :

    a. Dans le fichier de métadonnées SAML d'IAM Identity Center, choisissez Télécharger pour télécharger les métadonnées du fournisseur d'identité.

    b. Sous le certificat IAM Identity Center, choisissez Télécharger pour télécharger le certificat du fournisseur d'identité.

    > **Note**
    >
    > Vous aurez besoin de ces fichiers par la suite pour configurer l'application personnalisée sur le site web du fournisseur de services.

10. (Facultatif) Sous Propriétés de l'application, vous pouvez également spécifier l'URL de démarrage de l'application, l'état du relais et la durée de la session. Pour plus d'informations, consultez Configuration des propriétés de l'application dans la console IAM Identity Center.
11. Sous Métadonnées de l'application, choisissez Tapez manuellement vos valeurs de métadonnées. Indiquez ensuite l'URL ACS de l'application et les valeurs d'audience SAML de l'application.
12. Sélectionnez Envoyer. Vous êtes redirigé vers la page de détails de l'application que vous venez d'ajouter.

Propagation d'identité approuvée entre applications

La propagation fiable des identités permet aux AWS services d'effectuer les opérations suivantes :

- Autorisez l'accès aux AWS ressources en fonction du contexte d'identité de l'utilisateur.
- Partagez en toute sécurité le contexte d'identité de l'utilisateur avec d'autres AWS services.

Ces fonctionnalités permettent de définir, d'accorder et de consigner plus facilement l'accès des utilisateurs.

Grâce à la propagation sécurisée des identités, un utilisateur peut se connecter à une application, et cette application peut transmettre le contexte d'identité des utilisateurs dans les demandes d'accès aux données AWS des services. L'accès étant géré en fonction de l'identité de l'utilisateur, les utilisateurs n'ont pas besoin d'utiliser les informations d'identification utilisateur locales de la base de données ni d'assumer un rôle IAM pour accéder aux données.

Rubriques

Vue d'ensemble de la propagation d'identités fiables

Grâce à la propagation fiable des identités, l'accès AWS des utilisateurs aux ressources peut être défini, accordé et enregistré plus facilement. La propagation fiable des identités repose sur le cadre d'autorisation OAuth 2.0, qui permet aux applications d'accéder aux données des utilisateurs et de les partager en toute sécurité sans partager de mots de passe. OAuth 2.0 fournit un accès délégué sécurisé aux ressources de l'application. L'accès est délégué parce que l'administrateur des ressources approuve ou délègue l'application à laquelle l'utilisateur se connecte pour accéder à l'autre application.

Pour éviter de partager les mots de passe des utilisateurs, la propagation sécurisée des identités utilise des jetons. Les jetons constituent un moyen standard pour une application fiable de revendiquer qui est l'utilisateur et quelles demandes sont autorisées entre deux applications. AWS les applications gérées qui s'intègrent à une propagation d'identité fiable obtiennent des jetons directement auprès d'IAM Identity Center. IAM Identity Center permet également aux applications d'échanger des jetons d'identité et des jetons d'accès provenant d'un serveur d'autorisation OAuth 2.0 externe. Cela permet à une application de s'authentifier et d'obtenir des jetons en dehors de AWS, d'échanger le jeton contre un jeton IAM Identity Center et d'utiliser le nouveau jeton pour envoyer des demandes aux AWS services. Pour plus d'informations, consultez Utilisation d'applications dotées d'un émetteur de jetons fiable.

Le processus OAuth 2.0 démarre lorsqu'un utilisateur se connecte à une application. L'application à laquelle l'utilisateur se connecte lance une demande d'accès aux ressources de l'autre application. L'application initiatrice (demandeuse) peut accéder à l'application réceptrice au nom de l'utilisateur en demandant un jeton au serveur d'autorisation. Le serveur d'autorisation renvoie le jeton, et l'application initiatrice transmet ce jeton, avec une demande d'accès, à l'application réceptrice.

Cas d'utilisation de propagation d'identité fiables

En tant qu'administrateur du centre d'identité IAM, il peut vous être demandé d'aider à configurer une propagation d'identité fiable entre les applications initiatrices suivantes qui prennent en charge cette fonctionnalité et les AWS services connectés. Les sections suivantes fournissent des informations supplémentaires sur les cas d'utilisation spécifiques pris en charge par les applications qui peuvent initier la propagation d'identités fiables.

Rubriques

- Amazon EMR
- Amazon QuickSight
- Éditeur de requête Amazon Redshift v2
- Applications d'informatique décisionnelle tierces
- Applications développées sur mesure

Amazon EMR

Vous pouvez utiliser Amazon EMR comme application initiatrice pour les cas d'utilisation suivants relatifs à la propagation d'identités fiables.

Description	Autres AWS services utilisés	En savoir plus
Exécutez des analyses interactives avec Apache Spark sur Amazon EMR sur des clusters Amazon EC2 via Amazon EMR Studio. Appliquez un contrôle d'accès basé sur l'identité des employés et les attributs associés	Amazon EMR sur Amazon EC2 autorisé via AWS Lake Formation Amazon S3 Access Grants, Amazon S3, AWS Service Catalog	• Intégrez Amazon EMR à IAM Identity Center dans le guide de gestion Amazon EMR. • Les autorisations d'accès Amazon S3 et les identités des annuaires d'entreprise sont décrites dans le guide de

Description	Autres AWS services utilisés	En savoir plus
pour AWS Glue Catalog through AWS Lake Formation.	**Note** • Nécessite un accès via Amazon EMR Studio. • Contrôle d'accès au niveau de la table uniquement. • Apache Hive, PrestoSQL/ Trino et EMR Serverless ne sont pas pris en charge.	l'utilisateur d'Amazon Simple Storage Service. • Connexion AWS Lake Formation à IAM Identity Center dans le guide du AWS Lake Formation développeur • Utilisez votre identité d'entreprise à des fins d'analyse avec Amazon EMR et IAM Identity Center sur le blog Big Data AWS

Description	Autres AWS services utilisés	En savoir plus
Exécutez des analyses ad hoc avec Trino on Athena via Amazon EMR Studio. Appliquez un contrôle d'accès basé sur l'identité des employés et les attributs associés pour AWS Glue Catalog through AWS Lake Formation. Accès sécurisé à l'emplacement d'un compartiment de résultats de requête Athena dans Amazon S3 à l'aide d'Amazon S3 Access Grants.	Athena autorisée par le biais AWS Lake Formation d'Amazon S3 Access Grants **Note** Nécessite un accès via Amazon EMR Studio. L'accès direct depuis la Amazon Athena console n'est pas pris en charge.	• Intégrez Amazon EMR à IAM Identity Center dans le guide de gestion Amazon EMR. • L'utilisation d'IAM Identity Center a activé les groupes de travail Athena dans le guide de l'utilisateur d'Amazon Athena. • Les autorisations d'accès Amazon S3 et les identités des annuaires d'entreprise sont décrites dans le guide de l'utilisateur d'Amazon Simple Storage Service. • Connexion AWS Lake Formation à IAM Identity Center dans le guide du AWS Lake Formation développeur. • Communiquez l'identité de votre personnel à Amazon EMR Studio et à Athena sur le AWS blog Big Data.

Amazon QuickSight

Vous pouvez utiliser Amazon QuickSight comme application initiatrice pour les cas d'utilisation suivants relatifs à la propagation d'identités fiables.

Description	Autres AWS services utilisés	En savoir plus
QuickSight Les utilisateurs d'Amazon peuvent interroger	Amazon Redshift	• Connectez Redshift à IAM Identity Center pour offrir aux

Description	Autres AWS services utilisés	En savoir plus
les données Amazon Redshift. L'accès aux données est accordé dans Amazon Redshift par un administrateur Amazon Redshift.		utilisateurs une expérience d'authentification unique dans le guide de gestion Amazon Redshift. • Connectez Amazon Redshift à IAM Identity Center via Amazon QuickSight dans le guide de gestion Amazon Redshift.
QuickSight Les utilisateurs d'Amazon peuvent interroger Amazon Redshift Spectrum pour obtenir des données structurées dans Amazon S3, avec un accès autorisé par AWS Lake Formation un administrateur.	Amazon Redshift Spectrum, données structurées Amazon S3 *Par le biais d'Amazon Redshift Spectrum, autorisé par AWS Lake Formation	• Connectez Redshift à IAM Identity Center pour offrir aux utilisateurs une expérience d'authentification unique dans le guide de gestion Amazon Redshift. • Connectez Amazon Redshift à IAM Identity Center via Amazon QuickSight dans le guide de gestion Amazon Redshift. • Connexion AWS Lake Formation à IAM Identity Center dans le guide du AWS Lake Formation développeur. • Simplifiez la gestion des accès avec Amazon Redshift et AWS Lake Formation pour les utilisateurs via un fournisseur d'identité externe sur le blog AWS Big Data.

Description	Autres AWS services utilisés	En savoir plus
QuickSight Les utilisateurs d'Amazon peuvent interroge r les partages de données Amazon Redshift pour obtenir des données structurées dans Amazon S3, avec un accès autorisé par un administrateur. AWS Lake Formation	Partage de données Amazon Redshift, données structurées Amazon S3 *Par le biais d'Amazon Redshift, autorisé par AWS Lake Formation	• Connectez Amazon Redshift à IAM Identity Center via Amazon QuickSight dans le guide de gestion Amazon Redshift. • Connexion AWS Lake Formation à IAM Identity Center dans le guide du AWS Lake Formation développeur. • Simplifiez la gestion des accès avec Amazon Redshift et AWS Lake Formation pour les utilisateurs via un fournisseur d'identité externe sur le blog AWS Big Data.

Éditeur de requête Amazon Redshift v2

Vous pouvez utiliser l'éditeur de requêtes Amazon Redshift v2 comme application de lancement pour les cas d'utilisation suivants de propagation d'identités fiables.

Description	Autres AWS services utilisés	En savoir plus
Les utilisateurs de l'éditeur de requêtes Amazon Redshift v2 peuvent interroger les données Amazon Redshift. L'accès aux données est accordé dans Amazon Redshift par un administr ateur Amazon Redshift.	Amazon Redshift	• Connectez Redshift à IAM Identity Center pour offrir aux utilisateurs une expérience d'authentification unique dans le guide de gestion Amazon Redshift. • Connectez-vous à une base de données Amazon Redshift dans le guide de gestion Amazon Redshift.

Description	Autres AWS services utilisés	En savoir plus
		• OktaIntégrez Amazon Redshift Query Editor V2 à l'aide AWS IAM Identity Center d'une authentification unique fluide sur le blog AWS Big Data.
Les utilisateurs de l'éditeur de requêtes Amazon Redshift v2 peuvent interroger les tables externes Amazon Redshift Spectrum pour des données structurées dans Amazon S3, avec un accès autorisé par un administrateur. AWS Lake Formation	Amazon Redshift Spectrum, données structurées Amazon S3 *Par le biais d'Amazon Redshift Spectrum, autorisé par AWS Lake Formation	• Connectez Redshift à IAM Identity Center pour offrir aux utilisateurs une expérience d'authentification unique dans le guide de gestion Amazon Redshift. • Connectez-vous à une base de données Amazon Redshift dans le guide de gestion Amazon Redshift. • Connexion AWS Lake Formation à IAM Identity Center dans le guide du AWS Lake Formation développeur.
Les utilisateurs de l'éditeur de requêtes Amazon Redshift v2 peuvent interroger les partages de données Amazon Redshift avec un accès autorisé par un administrateur. AWS Lake Formation	partages de données Amazon Redshift, AWS Lake Formation	• Connectez-vous à une base de données Amazon Redshift dans le guide de gestion Amazon Redshift. • Connexion AWS Lake Formation à IAM Identity Center dans le guide du AWS Lake Formation développeur.

Applications d'informatique décisionnelle tierces

Vous pouvez utiliser une application d'informatique décisionnelle tierce, telle que Tableau, comme application de lancement pour des cas d'utilisation spécifiques de propagation d'identités fiables. Les applications de business intelligence tierces modifiées peuvent transmettre au pilote Amazon Redshift l'identité d'un utilisateur via des jetons d'identité ou des jetons d'accès OAuth, afin de demander des données à Amazon Redshift, avec un accès autorisé par un administrateur Amazon Redshift.

Applications développées sur mesure

Vous pouvez utiliser vos propres applications développées sur mesure comme application de lancement pour les cas d'utilisation suivants de propagation d'identité fiable.

Description	Autres AWS services utilisés	En savoir plus
Créez une application qui authentifie les utilisateurs via un serveur d'autorisation OAuth, puis utilisez AWS IAM Identity Center et IAM pour obtenir des informations d'identification de rôle IAM améliorées. Ces informations d'identification sont utilisées pour demander l'accès à des données non structurées dans Amazon S3, avec un accès autorisé par un administrateur Amazon S3 Access Grants.	AWS IAM Identity Center, données non structurées Amazon S3 *Autorisé par le biais d'Amazon S3 Access Grants	• Les autorisations d'accès Amazon S3 et les identités des annuaires d'entreprise sont décrites dans le guide de l'utilisateur d'Amazon Simple Storage Service. • Comment développer une application de données destinée aux utilisateurs avec IAM Identity Center et Amazon S3 Access Grants (partie 1) et (partie 2) dans le blog sur le AWS stockage.
Créez une application personnalisée qui interagit avec Amazon Q Business pour répondre aux questions des utilisateurs en fonction de votre propre contenu et des autorisations de l'utilisateur.	Centre d'identité IAM, Amazon Q Business	• Activez et configurez une instance IAM Identity Center dans le guide de l'utilisateur Amazon Q Business. • Comment utiliser les applications AWS gérées avec IAM

Description	Autres AWS services utilisés	En savoir plus
		Identity Center : activez Amazon Q sans migrer les flux de fédération IAM existants dans le blog sur la AWS sécurité.

Configurer une propagation d'identité fiable

La propagation d'identités fiables permet aux applications de s'authentifier de différentes manières afin de transmettre l'identité d'un utilisateur aux AWS services. La configuration pour la propagation d'identités fiables varie en fonction des types d'applications et de la manière dont elles s'authentifient.

> **Note**
>
> Vous devez configurer un émetteur de jetons de confiance si vous avez des applications gérées par des clients qui demandent l'accès à des applications AWS gérées, mais n'utilisent pas d' AWS API pour se connecter.

Rubriques

- Prérequis et considérations
- Utilisation d'une propagation d'identité fiable avec des applications AWS gérées
- Utilisation d'une propagation d'identité fiable avec des applications gérées par le client

Prérequis et considérations

Avant de configurer la propagation sécurisée des identités, passez en revue les conditions préalables et les considérations suivantes.

Rubriques

- Prérequis
- Considérations supplémentaires

Prérequis

Pour utiliser la propagation d'identité sécurisée, assurez-vous que votre environnement répond aux conditions préalables suivantes.

- Déploiement d'IAM Identity Center avec des utilisateurs et des groupes provisionnés

  Pour utiliser la propagation d'identité sécurisée, vous devez activer IAM Identity Center et configurer les utilisateurs et les groupes. Pour plus d'informations, veuillez consulter Démarrez avec les tâches courantes dans IAM Identity Center.

  Instance d'organisation recommandée — Nous vous recommandons d'utiliser une instance d'organisation d'IAM Identity Center que vous activez dans le compte de gestion d' AWS Organizations. Si vous envisagez d'utiliser la propagation d'identité sécurisée pour permettre aux utilisateurs d'accéder aux AWS services et aux ressources connexes dans différents domaines Comptes AWS au sein d'une même organisation, vous pouvez déléguer l'administration de votre instance d'IAM Identity Center à un compte membre.

  Si vous envisagez d'utiliser une instance à compte unique d'IAM Identity Center, tous les AWS services et ressources auxquels vous souhaitez que les utilisateurs accèdent par le biais d'une propagation d'identité sécurisée doivent résider dans le même appareil autonome Compte AWS ou dans le même compte membre de l'organisation dans laquelle vous avez activé IAM Identity Center. Pour plus d'informations, consultez Instances de compte d'IAM Identity Center.
- Pour les applications AWS gérées ; connexion à IAM Identity Center

  Pour utiliser une propagation d'identité fiable, les applications AWS gérées doivent s'intégrer à IAM Identity Center.

Considérations supplémentaires

Tenez compte des considérations supplémentaires suivantes concernant l'utilisation de la propagation d'identité sécurisée.

- Ne modifiez pas le paramètre Exiger des attributions pour les applications AWS gérées

  AWS les applications gérées ont une configuration de paramètres par défaut qui détermine si des attributions sont requises pour les utilisateurs et les groupes. Nous vous recommandons de ne pas modifier ce paramètre. Même si vous avez configuré des autorisations détaillées qui permettent aux utilisateurs d'accéder à des ressources spécifiques, la modification du paramètre Exiger des

attributions peut entraîner un comportement inattendu, notamment une interruption de l'accès des utilisateurs à ces ressources.

- Les autorisations multi-comptes (ensembles d'autorisations) ne sont pas requises

  La propagation fiable des identités ne vous oblige pas à configurer des autorisations multi-comptes (ensembles d'autorisations). Vous pouvez activer IAM Identity Center et l'utiliser uniquement pour une propagation d'identité fiable.

Utilisation d'une propagation d'identité fiable avec des applications AWS gérées

La propagation fiable des identités permet à une application AWS gérée de demander l'accès aux données AWS des services pour le compte d'un utilisateur. La gestion de l'accès aux données est basée sur l'identité de l'utilisateur, de sorte que les administrateurs peuvent accorder l'accès en fonction de l'appartenance des utilisateurs et des groupes aux utilisateurs existants. L'identité de l'utilisateur, les actions effectuées en son nom et les autres événements sont enregistrés dans des journaux et CloudTrail des événements spécifiques au service.

La propagation d'identités fiables est basée sur la norme OAuth 2.0. Pour utiliser cette fonctionnalité, les applications AWS gérées doivent s'intégrer à IAM Identity Center. AWS les services d'analyse peuvent fournir des interfaces basées sur des pilotes qui permettent à une application compatible d'utiliser une propagation d'identité fiable. Par exemple, les pilotes JDBC, ODBC et Python permettent aux outils de requête compatibles d'utiliser une propagation d'identité fiable sans que vous ayez à effectuer d'étapes de configuration supplémentaires.

Rubriques

- Configurez des applications AWS gérées pour une propagation d'identité fiable
- Flux de demandes de propagation d'identité fiables pour les applications AWS gérées
- Après l'obtention d'un jeton par une application
- Sessions de rôles IAM améliorées
- Types de sessions de rôle IAM à identité améliorée
- Processus de configuration et flux de demandes pour les applications AWS gérées

Configurez des applications AWS gérées pour une propagation d'identité fiable

AWS les services qui prennent en charge la propagation fiable des identités fournissent une interface utilisateur administrative et des API que vous pouvez utiliser pour configurer cette fonctionnalité. Aucune configuration n'est requise dans IAM Identity Center pour ces services.

Vous trouverez ci-dessous le processus de haut niveau pour configurer un AWS service de propagation d'identité fiable. Les étapes spécifiques varient en fonction de l'interface administrative et des API fournies par l'application.

1. Utilisez la console de l'application ou les API pour connecter l'application à votre instance d'IAM Identity Center

   Utilisez la console de l'application AWS gérée ou les API de l'application pour connecter l'application à votre instance d'IAM Identity Center. Lorsque vous utilisez la console pour l'application, l'interface utilisateur administrative inclut un widget qui rationalise le processus de configuration et de connexion.
2. Utiliser la console de l'application ou les API pour configurer l'accès des utilisateurs aux ressources de l'application

   Effectuez cette étape pour autoriser les ressources ou les données auxquelles un utilisateur peut accéder. L'accès dépend de l'identité de l'utilisateur ou de son appartenance à un groupe. Le modèle d'autorisation varie en fonction de l'application.

   > **Important**
   >
   > Vous devez effectuer cette étape pour permettre aux utilisateurs d'accéder aux ressources du AWS service. Dans le cas contraire, les utilisateurs ne peuvent pas accéder aux ressources, même si l'application demandeuse est autorisée à demander l'accès au service.

Flux de demandes de propagation d'identité fiables pour les applications AWS gérées

Tous les flux de propagation d'identités fiables vers les applications AWS gérées doivent commencer par une application qui obtient un jeton auprès d'IAM Identity Center. Ce jeton est obligatoire car il contient une référence à un utilisateur connu d'IAM Identity Center et aux applications enregistrées auprès d'IAM Identity Center.

Les sections suivantes décrivent comment une application AWS gérée peut obtenir un jeton auprès d'IAM Identity Center pour lancer une propagation d'identité fiable.

Rubriques

- Authentification basée sur le Web avec IAM Identity Center
- Demandes d'authentification basées sur la console et initiées par l'utilisateur

Authentification basée sur le Web avec IAM Identity Center

Pour ce flux, l'application AWS gérée fournit une expérience d'authentification unique basée sur le Web à l'aide d'IAM Identity Center pour l'authentification.

Lorsqu'un utilisateur ouvre une application AWS gérée, un flux d'authentification unique utilisant IAM Identity Center est déclenché. Si aucune session n'est active pour l'utilisateur dans IAM Identity Center, une page de connexion est présentée à l'utilisateur en fonction de la source d'identité que vous avez spécifiée, et IAM Identity Center crée une session pour l'utilisateur.

IAM Identity Center fournit AWS à l'application gérée un jeton qui inclut l'identité de l'utilisateur et une liste des audiences (Auds) et des étendues associées que l'application est enregistrée pour utiliser. L'application peut ensuite utiliser le jeton pour envoyer des demandes à d'autres AWS services de réception.

Demandes d'authentification basées sur la console et initiées par l'utilisateur

Pour ce flux, l'application AWS gérée fournit une expérience de console initiée par les utilisateurs.

Dans ce cas, l'application AWS gérée est saisie depuis la console de AWS gestion après avoir assumé un rôle. Pour que l'application obtienne un jeton, l'utilisateur doit lancer un processus pour déclencher l'authentification de l'utilisateur par l'application. Cela initie l'authentification à l'aide d'IAM Identity Center, qui redirige l'utilisateur vers la source d'identité que vous avez configurée.

Après l'obtention d'un jeton par une application

Une fois qu'une application demandeuse a obtenu un jeton auprès d'IAM Identity Center, l'application actualise régulièrement le jeton, qui peut être utilisé pendant toute la durée de la session de l'utilisateur. Pendant ce temps, l'application peut :

- Obtenez plus d'informations sur le jeton afin de déterminer qui est l'utilisateur et quelles étendues l'application peut utiliser avec d'autres applications AWS gérées réceptrices.

- Transmettez le jeton dans les appels à d'autres applications AWS gérées réceptrices qui prennent en charge l'utilisation de jetons.
- Obtenez des sessions de rôle IAM à identité améliorée qu'il peut utiliser pour envoyer des demandes à d'autres applications AWS gérées qui utilisent AWS Signature Version 4.

  Une session de rôle IAM améliorée est une session de rôle IAM qui contient l'identité propagée de l'utilisateur stockée dans un jeton créé par IAM Identity Center.

Sessions de rôles IAM améliorées

AWS Security Token Service Permet à une application d'obtenir une session de rôle IAM améliorée en termes d'identité. AWS les applications gérées qui prennent en charge le contexte utilisateur dans une session de rôle peuvent utiliser les informations d'identité pour autoriser l'accès en fonction de l'utilisateur participant à la session de rôle. Ce nouveau contexte permet aux applications d'envoyer des demandes aux applications AWS gérées qui prennent en charge la propagation d'identités fiables par le biais de demandes d'API AWS Signature Version 4.

Lorsqu'une application AWS gérée utilise une session de rôle IAM améliorée pour accéder à une ressource, elle CloudTrail enregistre l'identité de l'utilisateur (ID utilisateur), la session initiatrice et l'action entreprise.

Lorsqu'une application envoie une demande à l'aide d'une session de rôle IAM à identité améliorée à une application réceptrice, elle ajoute un contexte à la session afin que l'application réceptrice puisse autoriser l'accès en fonction de l'identité de l'utilisateur ou de son appartenance à un groupe, ou du rôle IAM. Les applications réceptrices qui prennent en charge la propagation sécurisée des identités renvoient une erreur si l'application réceptrice ou la ressource demandée n'est pas configurée pour autoriser l'accès en fonction de l'identité de l'utilisateur ou de son appartenance à un groupe.

Pour éviter ce problème, effectuez l'une des opérations suivantes :

- Vérifiez que l'application réceptrice est connectée à IAM Identity Center.
- Utilisez la console de l'application réceptrice ou les API de l'application pour configurer l'application afin d'autoriser l'accès aux ressources en fonction de l'identité de l'utilisateur ou de son appartenance à un groupe. Les exigences de configuration pour cela varient en fonction de l'application.

Pour plus d'informations, consultez la documentation de l'application AWS gérée réceptrice.

Types de sessions de rôle IAM à identité améliorée

Une application obtient une session de rôle IAM améliorée en envoyant une demande à l' AWS STS `AssumeRole`API et en transmettant une assertion de contexte dans le `ProvidedContexts` paramètre de la demande. `AssumeRole` L'assertion de contexte est obtenue à partir de la `idToken` réclamation disponible dans la réponse à la `SSO OIDC` `CreateTokenWithIAM` demande.

AWS STS peut créer deux types différents de sessions de rôle IAM à identité améliorée, en fonction de l'assertion de contexte fournie à la demande : `AssumeRole`

- Sessions dans lesquelles l'identité de l'utilisateur est enregistrée uniquement CloudTrail.
- Sessions qui activent l'autorisation en fonction de l'identité de l'utilisateur propagée et auxquelles elle se CloudTrail connecte.

Pour obtenir une session de rôle IAM à identité améliorée AWS STS fournissant uniquement des informations d'audit enregistrées dans un journal, CloudTrail indiquez la valeur de la `sts:audit_context` réclamation dans la demande. `AssumeRole` Pour obtenir une session qui autorise également le AWS service récepteur à autoriser l'utilisateur du IAM Identity Center à effectuer une action, indiquez la valeur de la `sts:identity_context` réclamation dans la `AssumeRole` demande. Vous ne pouvez fournir qu'un seul contexte.

Sessions de rôle IAM à identité améliorée créées avec **`sts:audit_context`**

Lorsqu'une demande est adressée à un AWS service à l'aide d'une session de rôle IAM améliorée créée avec`sts:audit_context`, le centre d'identité IAM de l'utilisateur `userId` est connecté à CloudTrail l'élément. `OnBehalfOf`

```
"userIdentity": {
      "type": "AssumedRole",
      "principalId": "AROAEXAMPLE:MyRole",
      "arn": "arn:aws:sts::111111111111:assumed-role/MyRole/MySession",
      "accountId": "111111111111",
      "accessKeyId": "ASIAEXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "AROAEXAMPLE",
            "arn": "arn:aws:iam::111111111111:role/MyRole",
            "accountId": "111111111111",
            "userName": "MyRole"
```

```
        },
        "attributes": {
            "creationDate": "2023-12-12T13:55:22Z",
            "mfaAuthenticated": "false"
        }
    },
    "onBehalfOf": {
        "userId": "11111111-1111-1111-1111-1111111111",
        "identityStoreArn": "arn:aws:identitystore::111111111111:identitystore/
d-111111111"
    }
}
```

> **Note**
>
> Ces sessions ne peuvent pas être utilisées pour autoriser l'utilisateur d'Identity Center. Ils peuvent toujours être utilisés pour autoriser le rôle IAM.

Pour obtenir ce type de session de rôle AWS STS, fournissez la valeur du `sts:audit_context` champ à la `AssumeRole` demande dans le paramètre de `ProvidedContexts` demande. Utilisez `arn:aws:iam::aws:contextProvider/IdentityStore` comme valeur pour`ProviderArn`.

Sessions de rôle IAM à identité améliorée créées avec **`sts:identity_context`**

Lorsqu'un utilisateur adresse une demande à un AWS service à l'aide d'une session de rôle IAM améliorée créée avec`sts:identity_context`, le centre d'identité IAM de l'utilisateur `userId` est connecté CloudTrail à l'`onBehalfOf`élément de la même manière qu'une session créée avec. `sts:audit_context`

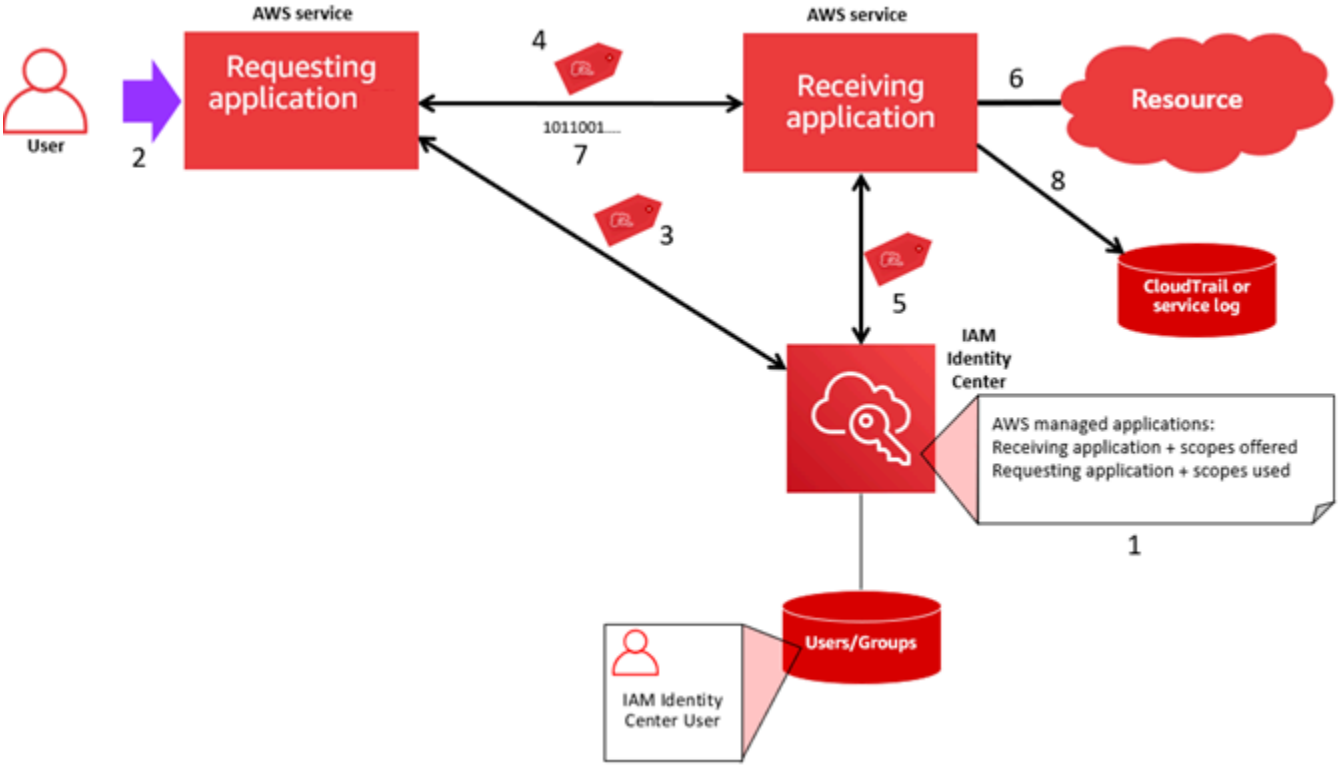
Outre la connexion de l'utilisateur à l'IAM Identity Center CloudTrail, ce type de session est également utilisé par les API prises en charge pour autoriser des actions en fonction de l'identité utilisateur propagée. `userId` Pour obtenir la liste des actions IAM pour les API prises en charge, consultez la politique `AWSIAMIdentityCenterAllowListForIdentityContext` AWS gérée. Cette stratégie AWS gérée est fournie en tant que stratégie de session lorsqu'une session de rôle IAM à identité améliorée est créée avec. `sts:identity_context` La politique vous empêche d'utiliser la session de rôle avec des AWS services non pris en charge.

Pour obtenir ce type de session de rôle AWS STS, fournissez la valeur du `sts:identity_context` champ à la `AssumeRole` demande dans le paramètre de `ProvidedContexts` demande. Utilisez `arn:aws:iam::aws:contextProvider/IdentityStore` comme valeur pour`ProviderArn`.

Processus de configuration et flux de demandes pour les applications AWS gérées

Cette section décrit le processus de configuration et le flux de demandes pour les applications AWS gérées qui utilisent une propagation d'identité fiable et qui fournissent une expérience d'authentification unique basée sur le Web.

Le schéma suivant donne un aperçu de ce processus.



Les étapes suivantes fournissent des informations supplémentaires sur ce processus.

1. Utilisez la console de l'application AWS gérée ou les API de l'application pour effectuer les opérations suivantes :
   a. Connectez l'application à votre instance d'IAM Identity Center.
   b. Configurez des autorisations pour autoriser les ressources d'application auxquelles un utilisateur peut accéder.
2. Le flux de demandes commence lorsqu'un utilisateur ouvre une application AWS gérée qui peut demander l'accès aux ressources (une application demandeuse).

3. Pour obtenir un jeton permettant d'accéder à l'application AWS gérée réceptrice, l'application AWS gérée demandeuse lance une demande de connexion à IAM Identity Center.

   Si l'utilisateur n'est pas connecté, IAM Identity Center déclenche un flux d'authentification utilisateur vers la source d'identité que vous avez spécifiée. Cela crée une nouvelle session de portail AWS d'accès pour l'utilisateur dont la durée est celle que vous avez configurée dans IAM Identity Center. IAM Identity Center génère ensuite un jeton associé à la session, et l'application peut fonctionner pendant la durée restante de la session du portail d' AWS accès de l'utilisateur. Si l'utilisateur se déconnecte de son application ou si vous supprimez sa session, celle-ci se termine automatiquement dans les deux heures.
4. L'application AWS gérée lance une demande à l'application réceptrice et fournit son jeton.
5. L'application réceptrice appelle IAM Identity Center pour obtenir l'identité de l'utilisateur et les étendues codées dans le jeton. L'application réceptrice peut également faire des demandes pour obtenir les attributs des utilisateurs ou les appartenances à des groupes d'utilisateurs à partir du répertoire Identity Center.
6. L'application réceptrice utilise sa configuration d'autorisation pour déterminer si l'utilisateur est autorisé à accéder à la ressource d'application demandée.
7. Si l'utilisateur est autorisé à accéder à la ressource d'application demandée, l'application réceptrice répond à la demande.
8. L'identité de l'utilisateur, les actions effectuées en son nom et les autres événements enregistrés dans les journaux et AWS CloudTrail événements de l'application réceptrice. La manière spécifique dont ces informations sont enregistrées varie en fonction de l'application.

Utilisation d'une propagation d'identité fiable avec des applications gérées par le client

La propagation fiable des identités permet à une application gérée par le client de demander l'accès aux données AWS des services au nom d'un utilisateur. La gestion de l'accès aux données est basée sur l'identité de l'utilisateur, de sorte que les administrateurs peuvent accorder l'accès en fonction de l'appartenance des utilisateurs et des groupes aux utilisateurs existants. L'identité de l'utilisateur, les actions effectuées en son nom et les autres événements sont enregistrés dans des journaux et CloudTrail des événements spécifiques au service.

Grâce à la propagation sécurisée des identités, un utilisateur peut se connecter à une application gérée par le client, et cette application peut transmettre l'identité de l'utilisateur dans les demandes d'accès aux données AWS des services.

> **Important**
>
> Pour accéder à un AWS service, les applications gérées par le client doivent obtenir un jeton auprès d'un émetteur de jetons fiable, externe à IAM Identity Center. Un émetteur de jetons de confiance est un serveur d'autorisation OAuth 2.0 qui crée des jetons signés. Ces jetons autorisent les applications qui lancent des demandes d'accès aux AWS services (réception d'applications). Pour plus d'informations, consultez Utilisation d'applications dotées d'un émetteur de jetons fiable.

Rubriques

Configurez des applications OAuth 2.0 gérées par le client pour une propagation d'identité fiable

Pour configurer une application OAuth 2.0 gérée par le client pour une propagation d'identité fiable, vous devez d'abord l'ajouter à IAM Identity Center. Utilisez la procédure suivante pour ajouter votre application à IAM Identity Center.

Rubriques

Étape 1 : Sélectionnez le type de demande

1. Ouvrez la console IAM Identity Center.
2. Choisissez Applications.
3. Choisissez l'onglet Géré par le client.
4. Choisissez Add application (Ajouter une application).
5. Sur la page Sélectionner le type d'application, sous Préférences de configuration, choisissez J'ai une application que je souhaite configurer.

6. Sous Type d'application, choisissez OAuth 2.0.
7. Choisissez Next pour passer à la page suivante,Étape 2 : Spécifier les détails de l'application.

Étape 2 : Spécifier les détails de l'application

1. Sur la page Spécifier les détails de l'application, sous Nom et description de l'application, entrez un nom d'affichage pour l'application, tel que**MyApp**. Entrez ensuite une description.
2. Sous Méthode d'attribution des utilisateurs et des groupes, choisissez l'une des options suivantes :

   - Exiger des attributions : autorisez uniquement les utilisateurs et les groupes IAM Identity Center affectés à cette application à accéder à l'application.

     Visibilité de la vignette de l'application : seuls les utilisateurs affectés à l'application directement ou par le biais d'une attribution de groupe peuvent voir la vignette de l'application dans le portail AWS d'accès, à condition que la visibilité de l'application dans le portail AWS d'accès soit définie sur Visible.
   - Pas besoin d'assignations : autorisez tous les utilisateurs et groupes autorisés d'IAM Identity Center à accéder à cette application.

     Visibilité de la vignette de l'application : la vignette de l'application est visible par tous les utilisateurs qui se connectent au portail AWS d'accès, sauf si la visibilité de l'application dans le portail d' AWS accès est définie sur Non visible.
3. Sous portail AWS d'accès, entrez l'URL à laquelle les utilisateurs peuvent accéder à l'application et spécifiez si la vignette de l'application sera visible ou non dans le portail AWS d'accès. Si vous choisissez Non visible, même les utilisateurs assignés ne peuvent pas voir la vignette de l'application.
4. Sous Balises (facultatif), choisissez Ajouter une nouvelle balise, puis spécifiez les valeurs de clé et de valeur (facultatif).

   Pour plus d'informations sur les balises, consultez Balisage de ressources AWS IAM Identity Center.
5. Choisissez Next, puis passez à la page suivante,Étape 3 : Spécifier les paramètres d'authentification.

Étape 3 : Spécifier les paramètres d'authentification

Pour ajouter une application gérée par le client qui prend en charge OAuth 2.0 à IAM Identity Center, vous devez spécifier un émetteur de jetons fiable. Un émetteur de jetons de confiance est un serveur d'autorisation OAuth 2.0 qui crée des jetons signés. Ces jetons autorisent les applications qui lancent des demandes (demandes d'applications) pour accéder aux applications AWS gérées (réception d'applications).

1. Sur la page Spécifier les paramètres d'authentification, sous Émetteurs de jetons fiables, effectuez l'une des opérations suivantes :

   - Pour utiliser un émetteur de jetons de confiance existant :

     Cochez la case à côté du nom de l'émetteur de jetons de confiance que vous souhaitez utiliser.

   - Pour ajouter un nouvel émetteur de jetons de confiance :

     1. Choisissez Créer un émetteur de jetons de confiance.
     2. Un nouvel onglet de navigateur s'ouvre. Suivez les étapes 5 à 8 dansComment ajouter un émetteur de jetons fiable à la console IAM Identity Center.
     3. Après avoir effectué ces étapes, retournez dans la fenêtre du navigateur que vous utilisez pour configurer votre application et sélectionnez l'émetteur de jetons de confiance que vous venez d'ajouter.
     4. Dans la liste des émetteurs de jetons de confiance, cochez la case à côté du nom de l'émetteur de jetons de confiance que vous venez d'ajouter.

        Une fois que vous avez sélectionné un émetteur de jetons de confiance, la section Configurer les émetteurs de jetons de confiance sélectionnés apparaît.

2. Sous Configurer les émetteurs de jetons fiables sélectionnés, entrez la réclamation Aud. La réclamation Aud identifie le public cible (destinataires) du jeton généré par l'émetteur de confiance. Pour plus d'informations, consultez Réclamation d'aide.
3. Pour éviter que vos utilisateurs n'aient à s'authentifier à nouveau lorsqu'ils utilisent cette application, sélectionnez Actualiser automatiquement l'authentification utilisateur pour une session d'application active. Lorsqu'elle est sélectionnée, cette option actualise le jeton d'accès à la session toutes les 60 minutes, jusqu'à ce que la session expire ou que l'utilisateur y mette fin.
4. Choisissez Next, puis passez à la page suivante,Étape 4 : Spécifier les informations d'identification de l'application.

Étape 4 : Spécifier les informations d'identification de l'application

Suivez les étapes de cette procédure pour spécifier les informations d'identification que votre application utilise pour effectuer des actions d'échange de jetons avec des applications fiables. Ces informations d'identification sont utilisées dans une politique basée sur les ressources. La politique exige que vous spécifiiez un principal autorisé à effectuer les actions spécifiées dans la stratégie. Vous devez spécifier un principal, même si les applications fiables se trouvent dans les mêmes applications Compte AWS.

> **Note**
>
> Lorsque vous définissez des autorisations à l'aide de politiques, accordez uniquement les autorisations requises pour effectuer une tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège.

Cette politique exige que des `sso-oauth:CreateTokenWithIAM` mesures soient prises.

1. Sur la page Spécifier les informations d'identification de l'application, effectuez l'une des opérations suivantes :

   - Pour définir rapidement un ou plusieurs rôles IAM :

     1. Choisissez Entrez un ou plusieurs rôles IAM.
     2. Sous Enter IAM roles, spécifiez le Amazon Resource Name (ARN) d'un rôle IAM existant. Pour spécifier l'ARN, utilisez la syntaxe suivante. La partie de la région de l'ARN est vide, car les ressources IAM sont globales.

        ```
        arn:aws:iam::account:role/role-name-with-path
        ```

        Pour plus d'informations, consultez la section Accès entre comptes à l'aide de politiques basées sur les ressources et d'ARN IAM dans le guide de l'utilisateur.AWS Identity and Access Management

   - Pour modifier manuellement la politique (obligatoire si vous ne spécifiez pas d'informations AWS d'identification) :

     1. Sélectionnez Modifier la politique de l'application.
     2. Modifiez votre politique en tapant ou en collant du texte dans la zone de texte JSON.

3. Résolvez les avertissements de sécurité, les erreurs ou les avertissements généraux générés lors de la validation des politiques. Pour plus d'informations, consultez la section Validation des politiques IAM dans le guide de l'AWS Identity and Access Management utilisateur.

2. Choisissez Next et passez à la page suivante,Étape 5 : révision et configuration.

Étape 5 : révision et configuration

1. Sur la page Révision et configuration, passez en revue les choix que vous avez faits. Pour apporter des modifications, choisissez la section de configuration souhaitée, choisissez Modifier, puis apportez les modifications requises.
2. Lorsque vous avez terminé, choisissez Ajouter une application.
3. L'application que vous avez ajoutée apparaît dans la liste des applications gérées par le client.
4. Après avoir configuré votre application gérée par le client dans IAM Identity Center, vous devez spécifier un ou plusieurs AWS services, ou applications fiables, pour la propagation des identités. Cela permet aux utilisateurs de se connecter à votre application gérée par le client et d'accéder aux données de l'application sécurisée.

   Pour plus d'informations, consultez Spécifier les applications fiables .

Spécifier les applications fiables

Après avoir configuré votre application gérée par le client, vous devez spécifier un ou plusieurs AWS services fiables, ou applications fiables, pour la propagation des identités. Spécifiez un AWS service contenant des données auxquelles les utilisateurs de vos applications gérées par le client doivent accéder. Lorsque vos utilisateurs se connectent à votre application gérée par le client, cette application transmet l'identité de vos utilisateurs à l'application sécurisée.

Utilisez la procédure suivante pour sélectionner un service, puis spécifiez les applications individuelles à approuver pour ce service.

1. Ouvrez la console IAM Identity Center.
2. Choisissez Applications.
3. Choisissez l'onglet Géré par le client.

4. Dans la liste des applications gérées par le client, sélectionnez l'application OAuth 2.0 pour laquelle vous souhaitez lancer des demandes d'accès. Il s'agit de l'application à laquelle vos utilisateurs se connectent.
5. Sur la page Détails, sous Applications fiables pour la propagation des identités, sélectionnez Spécifier les applications fiables.
6. Sous Type d'installation, sélectionnez Applications individuelles et spécifiez l'accès, puis choisissez Suivant.
7. Sur la page Sélectionner un service, choisissez le AWS service qui possède des applications auxquelles votre application gérée par le client peut faire confiance pour la propagation des identités, puis choisissez Next.

   Le service que vous sélectionnez définit les applications fiables. Vous allez sélectionner les applications à l'étape suivante.
8. Sur la page Sélectionner des applications, choisissez Applications individuelles, cochez la case correspondant à chaque application pouvant recevoir des demandes d'accès, puis choisissez Suivant.
9. Sur la page Configurer l'accès, sous Méthode de configuration, effectuez l'une des opérations suivantes :

   - Sélectionnez l'accès par application : sélectionnez cette option pour configurer différents niveaux d'accès pour chaque application. Choisissez l'application pour laquelle vous souhaitez configurer le niveau d'accès, puis choisissez Modifier l'accès. Dans Niveau d'accès à appliquer, modifiez les niveaux d'accès selon vos besoins, puis choisissez Enregistrer les modifications.
   - Appliquer le même niveau d'accès à toutes les applications : sélectionnez cette option si vous n'avez pas besoin de configurer les niveaux d'accès pour chaque application.
10. Choisissez Suivant.
11. Sur la page Vérifier la configuration, passez en revue les choix que vous avez effectués. Pour apporter des modifications, choisissez la section de configuration souhaitée, choisissez Modifier l'accès, puis apportez les modifications requises.
12. Lorsque vous avez terminé, choisissez Trust applications.

Utilisation d'applications dotées d'un émetteur de jetons fiable

Les émetteurs de jetons fiables vous permettent d'utiliser la propagation d'identité fiable avec des applications qui s'authentifient en dehors de. AWS Avec des émetteurs de jetons fiables, vous pouvez autoriser ces applications à faire des demandes d'accès aux applications AWS gérées au nom de leurs utilisateurs.

Les rubriques suivantes décrivent le fonctionnement des émetteurs de jetons fiables et fournissent des conseils de configuration.

Rubriques

Vue d'ensemble des émetteurs de jetons fiables

La propagation d'identités fiables fournit un mécanisme qui permet aux applications qui s'authentifient AWS à l'extérieur de faire des demandes au nom de leurs utilisateurs en utilisant un émetteur de jetons fiable. Un émetteur de jetons de confiance est un serveur d'autorisation OAuth 2.0 qui crée des jetons signés. Ces jetons autorisent les applications qui initient des demandes (demandes d'applications) pour accéder aux AWS services (réception d'applications). Les applications demandeuses lancent des demandes d'accès au nom des utilisateurs authentifiés par l'émetteur de jetons de confiance. Les utilisateurs sont connus à la fois de l'émetteur du jeton sécurisé et de l'IAM Identity Center.

AWS les services qui reçoivent des demandes gèrent l'autorisation précise de leurs ressources en fonction de leurs utilisateurs et de leur appartenance au groupe, comme indiqué dans le répertoire Identity Center. AWS les services ne peuvent pas utiliser directement les jetons provenant de l'émetteur de jetons externe.

Pour résoudre ce problème, IAM Identity Center fournit à l'application demandeuse, ou à un AWS pilote utilisé par l'application demandeuse, un moyen d'échanger le jeton émis par l'émetteur du jeton approuvé contre un jeton généré par IAM Identity Center. Le jeton généré par IAM Identity Center fait référence à l'utilisateur IAM Identity Center correspondant. L'application demandeuse, ou le

pilote, utilise le nouveau jeton pour lancer une demande à l'application réceptrice. Étant donné que le nouveau jeton fait référence à l'utilisateur correspondant dans IAM Identity Center, l'application réceptrice peut autoriser l'accès demandé en fonction de l'utilisateur ou de son appartenance à un groupe tel que représenté dans IAM Identity Center.

> **Important**
>
> Le choix d'un serveur d'autorisation OAuth 2.0 à ajouter en tant qu'émetteur de jetons de confiance est une décision de sécurité qui nécessite un examen attentif. Choisissez uniquement des émetteurs de jetons fiables en qui vous avez confiance pour effectuer les tâches suivantes :
>
> - Authentifiez l'utilisateur indiqué dans le jeton.
> - Autorisez l'accès de cet utilisateur à l'application réceptrice.
> - Générez un jeton qu'IAM Identity Center peut échanger contre un jeton créé par IAM Identity Center.

Conditions préalables et considérations pour les émetteurs de jetons fiables

Avant de configurer un émetteur de jetons fiable, passez en revue les conditions préalables et les considérations suivantes.

- Configuration d'un émetteur de jetons fiable

  Vous devez configurer un serveur d'autorisation OAuth 2.0 (l'émetteur de jetons de confiance). Bien que l'émetteur de jetons de confiance soit généralement le fournisseur d'identité que vous utilisez comme source d'identité pour IAM Identity Center, il n'est pas nécessaire que ce soit le cas. Pour plus d'informations sur la configuration de l'émetteur de jetons de confiance, consultez la documentation du fournisseur d'identité concerné.

  > **Note**
  >
  > Vous pouvez configurer jusqu'à 10 émetteurs de jetons fiables à utiliser avec IAM Identity Center, à condition de mapper l'identité de chaque utilisateur de l'émetteur de jetons de confiance à un utilisateur correspondant dans IAM Identity Center.

- Le serveur d'autorisation OAuth 2.0 (l'émetteur de jetons de confiance) qui crée le jeton doit disposer d'un point de terminaison de découverte OpenID Connect (OIDC) que IAM Identity Center peut utiliser pour obtenir des clés publiques afin de vérifier les signatures des jetons. Pour plus d'informations, consultez URL du point de terminaison de découverte OIDC (URL de l'émetteur).
- Tokens émis par l'émetteur de jetons de confiance

  Les jetons émis par l'émetteur de jetons de confiance doivent répondre aux exigences suivantes :

  - Le jeton doit être signé et au format JSON Web Token (JWT) à l'aide de l'algorithme RS256.
  - Le jeton doit contenir les allégations suivantes :
    - Émetteur (iss) — Entité qui a émis le jeton. Cette valeur doit correspondre à la valeur configurée dans le point de terminaison de découverte OIDC (URL de l'émetteur) dans l'émetteur de jetons de confiance.
    - Sujet (sous) — L'utilisateur authentifié.
    - Audience (aud) — Destinataire prévu du jeton. Il s'agit du AWS service qui sera accessible une fois le jeton échangé contre un jeton auprès d'IAM Identity Center. Pour plus d'informations, consultez Réclamation d'aide.
    - Délai d'expiration (exp) : délai après lequel le jeton expire.
    -
  - Le jeton peut être un jeton d'identité ou un jeton d'accès.
  - Le jeton doit avoir un attribut qui peut être mappé de manière unique à un utilisateur du IAM Identity Center.
- Réclamations facultatives

  IAM Identity Center prend en charge toutes les revendications facultatives définies dans la RFC 7523. Pour plus d'informations, consultez la section 3 : Format JWT et exigences de traitement de cette RFC.

  Par exemple, le jeton peut contenir une réclamation JTI (JWT ID). Cette réclamation, lorsqu'elle est présente, empêche les jetons portant le même JTI d'être réutilisés pour des échanges de jetons. Pour plus d'informations sur les réclamations de la JTI, consultezDétails de la réclamation de JTI.
- Configuration du centre d'identité IAM pour fonctionner avec un émetteur de jetons fiable

  Vous devez également activer IAM Identity Center, configurer la source d'identité pour IAM Identity Center et configurer les utilisateurs correspondant aux utilisateurs figurant dans le répertoire de l'émetteur de jetons de confiance.

Pour ce faire, vous devez effectuer l'une des opérations suivantes :

- Synchronisez les utilisateurs dans IAM Identity Center à l'aide du protocole SCIM (System for Cross-Domain Identity Management) 2.0.
- Créez les utilisateurs directement dans IAM Identity Center.

> **Note**
>
> Les émetteurs de jetons fiables ne sont pas pris en charge si vous utilisez le service de domaine Active Directory comme source d'identité.

Détails de la réclamation de JTI

Si IAM Identity Center reçoit une demande d'échange d'un jeton qu'IAM Identity Center a déjà échangé, la demande échoue. Pour détecter et empêcher la réutilisation d'un jeton pour des échanges de jetons, vous pouvez inclure une réclamation JTI. IAM Identity Center protège contre la réédition de jetons en fonction des revendications contenues dans le jeton.

Tous les serveurs d'autorisation OAuth 2.0 n'ajoutent pas de revendication JTI aux jetons. Certains serveurs d'autorisation OAuth 2.0 peuvent ne pas vous autoriser à ajouter une JTI en tant que réclamation personnalisée. Les serveurs d'autorisation OAuth 2.0 qui prennent en charge l'utilisation d'une réclamation JTI peuvent ajouter cette réclamation uniquement aux jetons d'identité, aux jetons d'accès uniquement, ou aux deux. Pour plus d'informations, consultez la documentation de votre serveur d'autorisation OAuth 2.0.

Pour plus d'informations sur la création d'applications qui échangent des jetons, consultez la documentation de l'API IAM Identity Center. Pour plus d'informations sur la configuration d'une application gérée par le client afin d'obtenir et d'échanger les jetons appropriés, consultez la documentation de l'application.

Paramètres de configuration de l'émetteur de jetons fiables

Les sections suivantes décrivent les paramètres requis pour configurer et utiliser un émetteur de jetons fiable.

Rubriques

- Réclamation d'aide

URL du point de terminaison de découverte OIDC (URL de l'émetteur)

Lorsque vous ajoutez un émetteur de jetons fiable à la console IAM Identity Center, vous devez spécifier l'URL du point de terminaison de découverte OIDC. Cette URL est généralement désignée par son URL relative,`/.well-known/openid-configuration`. Dans la console IAM Identity Center, cette URL est appelée URL de l'émetteur.

> **Note**
>
> Vous devez coller l'URL du point de terminaison de découverte jusqu'au bout et sans `.well-known/openid-configuration`. Si elle `.well-known/openid-configuration` est incluse dans l'URL, la configuration de l'émetteur de jetons de confiance ne fonctionnera pas. Comme IAM Identity Center ne valide pas cette URL, si celle-ci n'est pas correctement formée, la configuration de l'émetteur de jetons de confiance échouera sans notification.

IAM Identity Center utilise cette URL pour obtenir des informations supplémentaires sur l'émetteur du jeton de confiance. Par exemple, IAM Identity Center utilise cette URL pour obtenir les informations requises pour vérifier les jetons générés par l'émetteur de jetons de confiance. Lorsque vous ajoutez un émetteur de jetons de confiance à IAM Identity Center, vous devez spécifier cette URL. Pour trouver l'URL, consultez la documentation du fournisseur de serveur d'autorisation OAuth 2.0 que vous utilisez pour générer des jetons pour votre application, ou contactez directement le fournisseur pour obtenir de l'aide.

Mappage d'attribut

Les mappages d'attributs permettent à IAM Identity Center de faire correspondre l'utilisateur représenté dans un jeton émis par un émetteur de jeton fiable à un seul utilisateur dans IAM Identity Center. Vous devez spécifier le mappage des attributs lorsque vous ajoutez l'émetteur de jetons de confiance à IAM Identity Center. Ce mappage d'attributs est utilisé dans une réclamation dans le jeton généré par l'émetteur du jeton fiable. La valeur de la réclamation est utilisée pour effectuer une recherche dans IAM Identity Center. La recherche utilise l'attribut spécifié pour récupérer un seul utilisateur dans IAM Identity Center, qui sera utilisé comme utilisateur dans AWS le centre. La réclamation que vous choisissez doit être mappée à un attribut dans une liste fixe d'attributs disponibles dans la banque d'identités IAM Identity Center. Vous pouvez choisir l'un des attributs de la banque d'identités IAM Identity Center suivants : nom d'utilisateur, e-mail et identifiant externe.

La valeur de l'attribut que vous spécifiez dans IAM Identity Center doit être unique pour chaque utilisateur.

Réclamation d'aide

Une réclamation AUD identifie le public (destinataires) auquel un jeton est destiné. Lorsque l'application demandant l'accès s'authentifie via un fournisseur d'identité qui n'est pas fédéré à IAM Identity Center, ce fournisseur d'identité doit être configuré en tant qu'émetteur de jetons de confiance. L'application qui reçoit la demande d'accès (l'application réceptrice) doit échanger le jeton généré par l'émetteur du jeton approuvé contre un jeton généré par IAM Identity Center.

Pour plus d'informations sur la façon d'obtenir les valeurs de réclamation en dollars australiens pour l'application réceptrice telles qu'elles sont enregistrées auprès de l'émetteur de jetons de confiance, consultez la documentation de votre émetteur de jetons de confiance ou contactez l'administrateur de l'émetteur de jetons de confiance pour obtenir de l'aide.

Configuration d'un émetteur de jetons de confiance

Pour permettre la propagation d'identités fiables pour une application qui s'authentifie en externe auprès d'IAM Identity Center, un ou plusieurs administrateurs doivent configurer un émetteur de jetons fiable. Un émetteur de jetons de confiance est un serveur d'autorisation OAuth 2.0 qui émet des jetons aux applications qui initient des demandes (applications demandeuses). Les jetons autorisent ces applications à lancer des demandes au nom de leurs utilisateurs auprès d'une application réceptrice (un AWS service).

Rubriques

Coordination des rôles et responsabilités administratifs

Dans certains cas, un seul administrateur peut effectuer toutes les tâches nécessaires à la configuration d'un émetteur de jetons de confiance. Si plusieurs administrateurs exécutent

ces tâches, une étroite coordination est requise. Le tableau suivant décrit comment plusieurs administrateurs peuvent se coordonner pour configurer un émetteur de jetons fiable et configurer le AWS service pour l'utiliser.

> **Note**
>
> L'application peut être n'importe quel AWS service intégré à IAM Identity Center et prenant en charge la propagation fiable des identités.

Pour plus d'informations, consultez Tâches relatives à la configuration d'un émetteur de jetons de confiance.

Rôle	Effectue ces tâches	Se coordonne avec
Administrateur du centre d'identité IAM	Ajoute l'IdP externe en tant qu'émetteur de jetons de confiance à la console IAM Identity Center. Permet de configurer le mappage d'attributs correct entre IAM Identity Center et l'IdP externe. Informe l'administrateur du AWS service lorsque l'émetteur du jeton sécurisé est ajouté à la console IAM Identity Center.	Administrateur d'un IdP externe (émetteur de jetons de confiance) AWS administrateur de service
Administrateur d'un IdP externe (émetteur de jetons de confiance)	Configure l'IdP externe pour émettre des jetons. Permet de configurer le mappage d'attributs correct entre IAM Identity Center et l'IdP externe. Fournit le nom du public (réclamation Aud) à l'administrateur du AWS service.	Administrateur du centre d'identité IAM AWS administrateur de service

Rôle	Effectue ces tâches	Se coordonne avec
AWS administrateur de service	Vérifie la présence de l'émetteur de jetons de confiance dans la console de AWS service. L'émetteur du jeton sécurisé sera visible dans la console de AWS service une fois que l'administrateur d'IAM Identity Center l'aura ajouté à la console IAM Identity Center. Configure le AWS service pour qu'il utilise l'émetteur de jetons de confiance.	Administrateur du centre d'identité IAM Administrateur d'un IdP externe (émetteur de jetons de confiance)

Tâches relatives à la configuration d'un émetteur de jetons de confiance

Pour configurer un émetteur de jetons fiable, un administrateur du centre d'identité IAM, un administrateur d'IdP externe (émetteur de jetons de confiance) et un administrateur de l'application doivent effectuer les tâches suivantes.

> **Note**
>
> L'application peut être n'importe quel AWS service intégré à IAM Identity Center et prenant en charge la propagation fiable des identités.

1. Ajouter l'émetteur de jetons de confiance à IAM Identity Center : l'administrateur du centre d'identité d'IAM ajoute l'émetteur de jeton de confiance à l'aide de la console ou des API du centre d'identité d'IAM. Cette configuration nécessite de spécifier les éléments suivants :
   - Un nom pour l'émetteur de jetons de confiance
   - URL du point de terminaison de découverte OIDC (dans la console IAM Identity Center, cette URL est appelée URL de l'émetteur).
   - Mappage d'attributs pour la recherche par l'utilisateur. Ce mappage d'attributs est utilisé dans une réclamation dans le jeton généré par l'émetteur du jeton fiable. La valeur de la

réclamation est utilisée pour effectuer une recherche dans IAM Identity Center. La recherche utilise l'attribut spécifié pour récupérer un seul utilisateur dans IAM Identity Center.

2. Connecter le AWS service à IAM Identity Center : l'administrateur du AWS service doit connecter l'application à IAM Identity Center à l'aide de la console de l'application ou des API de l'application.

   Une fois que l'émetteur du jeton sécurisé est ajouté à la console IAM Identity Center, il est également visible dans la console de AWS service et peut être sélectionné par l'administrateur du AWS service.

3. Configurer l'utilisation de l'échange de jetons : dans la console de AWS service, l'administrateur du AWS service configure le AWS service pour accepter les jetons émis par l'émetteur de jetons de confiance. Ces jetons sont échangés contre des jetons générés par IAM Identity Center. Cela nécessite de spécifier le nom de l'émetteur de jetons de confiance indiqué à l'étape 1 et la valeur de réclamation Aud correspondant au AWS service.

   L'émetteur de jetons de confiance place la valeur de réclamation Aud dans le jeton qu'il émet pour indiquer que le jeton est destiné à être utilisé par le AWS service. Pour obtenir cette valeur, contactez l'administrateur de l'émetteur du jeton de confiance.

Comment ajouter un émetteur de jetons fiable à la console IAM Identity Center

Dans une organisation qui compte plusieurs administrateurs, cette tâche est exécutée par un administrateur du IAM Identity Center. Si vous êtes l'administrateur de l'IAM Identity Center, vous devez choisir l'IdP externe à utiliser comme émetteur de jetons de confiance.

Pour ajouter un émetteur de jetons fiable à la console IAM Identity Center

1. Ouvrez la console IAM Identity Center.
2. Sélectionnez Settings (Paramètres).
3. Sur la page Paramètres, choisissez l'onglet Authentification.
4. Sous Émetteurs de jetons fiables, choisissez Créer un émetteur de jetons de confiance.
5. Sur la page Configurer un IdP externe pour émettre des jetons fiables, sous Détails de l'émetteur de jetons fiables, procédez comme suit :

   - Pour l'URL de l'émetteur, spécifiez l'URL de découverte OIDC de l'IdP externe qui émettra des jetons pour une propagation d'identité fiable. Vous devez spécifier l'URL du point de

terminaison de découverte jusqu'au bout et sans `.well-known/openid-configuration`. L'administrateur de l'IdP externe peut fournir cette URL.

> **Note**
>
> Remarque Cette URL doit correspondre à l'URL figurant dans la réclamation de l'émetteur (iss) dans les jetons émis pour une propagation d'identité fiable.

- Pour Nom de l'émetteur de jeton fiable, entrez un nom pour identifier cet émetteur de jeton fiable dans IAM Identity Center et dans la console de l'application.

6. Sous Attributs de carte, procédez comme suit :

   - Pour l'attribut du fournisseur d'identité, sélectionnez un attribut dans la liste à mapper à un attribut de la banque d'identités IAM Identity Center.
   - Pour l'attribut IAM Identity Center, sélectionnez l'attribut correspondant pour le mappage des attributs.

7. Sous Tags (facultatif), choisissez Ajouter une nouvelle balise, spécifiez une valeur pour Key, et éventuellement pour Value.

   Pour plus d'informations sur les balises, consultez Balisage de ressources AWS IAM Identity Center.

8. Choisissez Créer un émetteur de jetons de confiance.
9. Une fois que vous avez créé l'émetteur de jetons de confiance, contactez l'administrateur de l'application pour lui communiquer le nom de l'émetteur de jeton de confiance, afin qu'il puisse confirmer que l'émetteur de jetons de confiance est visible dans la console appropriée.
10. L'administrateur de l'application doit sélectionner cet émetteur de jeton sécurisé dans la console applicable pour permettre aux utilisateurs d'accéder à l'application à partir d'applications configurées pour la propagation d'identités fiables.

Comment afficher ou modifier les paramètres de l'émetteur de jetons fiables dans la console IAM Identity Center

Après avoir ajouté un émetteur de jetons de confiance à la console IAM Identity Center, vous pouvez consulter et modifier les paramètres appropriés.

Si vous envisagez de modifier les paramètres de l'émetteur de jetons de confiance, gardez à l'esprit que les utilisateurs risquent de perdre l'accès à toutes les applications configurées pour utiliser

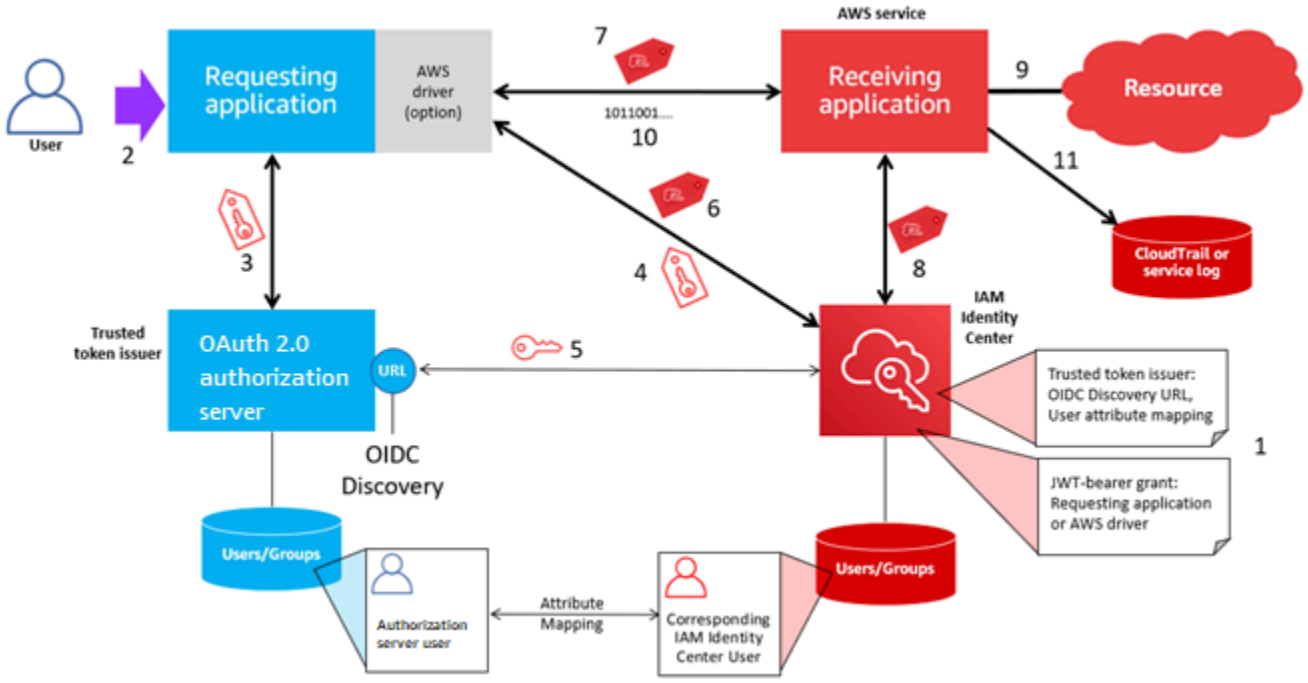
l'émetteur de jetons de confiance. Pour éviter de perturber l'accès des utilisateurs, nous vous recommandons de vous coordonner avec les administrateurs de toutes les applications configurées pour utiliser l'émetteur de jetons approuvé avant de modifier les paramètres.

Pour consulter ou modifier les paramètres de l'émetteur de jetons de confiance dans la console IAM Identity Center

1. Ouvrez la console IAM Identity Center.
2. Sélectionnez Settings (Paramètres).
3. Sur la page Paramètres, choisissez l'onglet Authentification.
4. Sous Émetteurs de jetons fiables, sélectionnez l'émetteur de jetons de confiance que vous souhaitez consulter ou modifier.
5. Sélectionnez Actions, puis Edit (Modifier).
6. Sur la page Modifier l'émetteur de jetons de confiance, consultez ou modifiez les paramètres selon vos besoins. Vous pouvez modifier le nom de l'émetteur du jeton fiable, les mappages d'attributs et les balises.
7. Sélectionnez Enregistrer les modifications.
8. Dans la boîte de dialogue Modifier l'émetteur de jetons de confiance, vous êtes invité à confirmer que vous souhaitez apporter des modifications. Choisissez Confirmer.

Processus de configuration et flux de demandes pour les applications utilisant un émetteur de jetons fiable

Cette section décrit le processus de configuration et le flux de demandes pour les applications qui utilisent un émetteur de jetons fiable pour la propagation d'identités fiables. Le schéma suivant donne un aperçu de ce processus.



Les étapes suivantes fournissent des informations supplémentaires sur ce processus.

1. Configurez IAM Identity Center et l'application AWS gérée réceptrice pour qu'ils utilisent un émetteur de jetons fiable. Pour plus d'informations, veuillez consulter Tâches relatives à la configuration d'un émetteur de jetons de confiance.
2. Le flux de demandes commence lorsqu'un utilisateur ouvre l'application demandeuse.
3. L'application demandeuse demande un jeton à l'émetteur de jetons de confiance pour initier des demandes à l'application AWS gérée réceptrice. Si l'utilisateur ne s'est pas encore authentifié, ce processus déclenche un flux d'authentification. Le jeton contient les informations suivantes :
   - Le sujet (Sub) de l'utilisateur.
   - Attribut utilisé par IAM Identity Center pour rechercher l'utilisateur correspondant dans IAM Identity Center.
   - Une réclamation d'audience (Aud) contenant une valeur que l'émetteur de jetons de confiance associe à l'application AWS gérée réceptrice. Si d'autres réclamations sont présentes, elles ne sont pas utilisées par IAM Identity Center.
4. L'application demandeuse, ou le AWS pilote qu'elle utilise, transmet le jeton à IAM Identity Center et demande que le jeton soit échangé contre un jeton généré par IAM Identity Center. Si vous utilisez un AWS pilote, vous devrez peut-être le configurer pour ce cas d'utilisation. Pour plus d'informations, consultez la documentation de l'application AWS gérée correspondante.

5. IAM Identity Center utilise le point de terminaison OIDC Discovery pour obtenir la clé publique qu'il peut utiliser pour vérifier l'authenticité du jeton. IAM Identity Center effectue ensuite les opérations suivantes :
   - Vérifie le jeton.
   - Effectue une recherche dans le répertoire Identity Center. Pour ce faire, IAM Identity Center utilise l'attribut mappé spécifié dans le jeton.
   - Vérifie que l'utilisateur est autorisé à accéder à l'application réceptrice. Si l'application AWS gérée est configurée pour exiger des affectations à des utilisateurs et à des groupes, l'utilisateur doit avoir une attribution directe ou basée sur un groupe à l'application ; sinon, la demande est refusée. Si l'application AWS gérée est configurée pour ne pas nécessiter d'assignation d'utilisateur ou de groupe, le traitement se poursuit.

     > **Note**
     >
     > AWS les services ont une configuration de paramètres par défaut qui détermine si des attributions sont requises pour les utilisateurs et les groupes. Nous vous recommandons de ne pas modifier le paramètre Exiger des attributions pour ces applications si vous prévoyez de les utiliser dans le cadre d'une propagation d'identité sécurisée. Même si vous avez configuré des autorisations détaillées qui permettent aux utilisateurs d'accéder à des ressources spécifiques de l'application, la modification du paramètre Exiger des attributions peut entraîner un comportement inattendu, notamment une interruption de l'accès des utilisateurs à ces ressources.

   - Vérifie que l'application demandeuse est configurée pour utiliser des étendues valides pour l'application AWS gérée réceptrice.
6. Si les étapes de vérification précédentes sont réussies, IAM Identity Center crée un nouveau jeton. Le nouveau jeton est un jeton opaque (crypté) qui inclut l'identité de l'utilisateur correspondant dans IAM Identity Center, le public (Aud) de l'application AWS gérée réceptrice et les étendues que l'application demandeuse peut utiliser lorsqu'elle adresse des demandes à l'application AWS gérée réceptrice.
7. L'application demandeuse, ou le pilote qu'elle utilise, lance une demande de ressource à l'application réceptrice et transmet le jeton généré par IAM Identity Center à l'application réceptrice.
8. L'application réceptrice appelle IAM Identity Center pour obtenir l'identité de l'utilisateur et les étendues codées dans le jeton. Il peut également faire des demandes pour obtenir les attributs des utilisateurs ou les appartenances à des groupes d'utilisateurs à partir du répertoire Identity Center.

9. L'application réceptrice utilise sa configuration d'autorisation pour déterminer si l'utilisateur est autorisé à accéder à la ressource d'application demandée.
10. Si l'utilisateur est autorisé à accéder à la ressource d'application demandée, l'application réceptrice répond à la demande.
11. L'identité de l'utilisateur, les actions effectuées en son nom et les autres événements enregistrés dans les journaux et CloudTrail événements de l'application réceptrice. La manière spécifique dont ces informations sont enregistrées varie en fonction de l'application.

Gérer les certificats IAM Identity Center

IAM Identity Center utilise des certificats pour établir une relation de confiance SAML entre IAM Identity Center et le fournisseur de services de votre application. Lorsque vous ajoutez une application dans IAM Identity Center, un certificat IAM Identity Center est automatiquement créé pour être utilisé avec cette application pendant le processus de configuration. Par défaut, ce certificat IAM Identity Center généré automatiquement est valide pour une période de cinq ans.

En tant qu'administrateur d'IAM Identity Center, vous devrez parfois remplacer les anciens certificats par des certificats plus récents pour une application donnée. Par exemple, il se peut que vous deviez remplacer un certificat lorsque sa date d'expiration approche. Le processus de remplacement d'un ancien certificat par un nouveau est appelé rotation des certificats.

Rubriques

Considérations à prendre en compte avant de faire pivoter

Avant de commencer le processus de rotation d'un certificat dans IAM Identity Center, tenez compte des points suivants :

- Le processus de rotation des certifications nécessite que vous rétablissiez la confiance entre IAM Identity Center et le fournisseur de services. Pour rétablir la confiance, utilisez les procédures fournies dansRotation d'un certificat IAM Identity Center.

- La mise à jour du certificat auprès du fournisseur de services peut entraîner une interruption de service temporaire pour vos utilisateurs jusqu'à ce que la confiance soit rétablie avec succès. Planifiez cette opération avec soin en dehors des heures de pointe si possible.

Rotation d'un certificat IAM Identity Center

La rotation d'un certificat IAM Identity Center est un processus en plusieurs étapes qui implique les étapes suivantes :

- Génération d'un nouveau certificat
- Ajouter le nouveau certificat sur le site Web du fournisseur de services
- Activer le nouveau certificat
- Supprimer le certificat inactif

Utilisez toutes les procédures suivantes dans l'ordre suivant pour terminer le processus de rotation des certificats pour une application donnée.

Étape 1 : Générez un nouveau certificat.

Les nouveaux certificats IAM Identity Center que vous générez peuvent être configurés pour utiliser les propriétés suivantes :

- Période de validité — Spécifie le temps imparti (en mois) avant l'expiration d'un nouveau certificat IAM Identity Center.
- Taille de clé — Détermine le nombre de bits qu'une clé doit utiliser avec son algorithme cryptographique. Vous pouvez définir cette valeur sur 1024 bits RSA ou 2048 bits RSA. Pour des informations générales sur le fonctionnement de la taille des clés en cryptographie, consultez la section Taille des clés.
- Algorithme — Spécifie l'algorithme utilisé par IAM Identity Center lors de la signature de l'assertion/réponse SAML. Vous pouvez définir cette valeur sur SHA-1 ou SHA-256. AWS recommande d'utiliser le protocole SHA-256 dans la mesure du possible, sauf si votre fournisseur de services exige le protocole SHA-1. Pour des informations générales sur le fonctionnement des algorithmes de cryptographie, voir Cryptographie à clé publique.

1. Ouvrez la console IAM Identity Center.
2. Choisissez Applications.

3. Dans la liste des applications, sélectionnez l'application pour laquelle vous souhaitez générer un nouveau certificat.
4. Sur la page des détails de l'application, choisissez l'onglet Configuration. Sous les métadonnées du centre d'identité IAM, sélectionnez Gérer le certificat. Si vous n'avez pas d'onglet Configuration ou si le paramètre de configuration n'est pas disponible, il n'est pas nécessaire de faire pivoter le certificat pour cette application.
5. Sur la page du certificat IAM Identity Center, sélectionnez Générer un nouveau certificat.
6. Dans la boîte de dialogue Générer un nouveau certificat IAM Identity Center, spécifiez les valeurs appropriées pour la période de validité, l'algorithme et la taille de la clé. Choisissez ensuite Generate.

Étape 2 : mettez à jour le site Web du fournisseur de services.

Suivez la procédure ci-dessous pour rétablir la confiance avec le fournisseur de services de l'application.

> **Important**
>
> Lorsque vous téléchargez le nouveau certificat auprès du fournisseur de services, il est possible que vos utilisateurs ne soient pas en mesure de s'authentifier. Pour corriger cette situation, définissez le nouveau certificat comme actif, comme décrit à l'étape suivante.

1. Dans la console IAM Identity Center, choisissez l'application pour laquelle vous venez de générer un nouveau certificat.
2. Sur la page des détails de l'application, choisissez Modifier la configuration.
3. Choisissez Afficher les instructions, puis suivez les instructions du site Web de votre fournisseur de services d'application spécifique pour ajouter le certificat nouvellement généré.

Étape 3 : Activez le nouveau certificat.

Jusqu'à deux certificats peuvent être attribués à une application. IAM Identity Center utilisera la certification définie comme active pour signer toutes les assertions SAML.

1. Ouvrez la console IAM Identity Center.
2. Choisissez Applications.

3. Dans la liste des applications, sélectionnez votre application.
4. Sur la page des détails de l'application, choisissez l'onglet Configuration. Sous les métadonnées du centre d'identité IAM, sélectionnez Gérer le certificat.
5. Sur la page du certificat IAM Identity Center, sélectionnez le certificat que vous souhaitez définir comme actif, choisissez Actions, puis sélectionnez Définir comme actif.
6. Dans la boîte de dialogue Définir le certificat sélectionné comme actif, confirmez que vous comprenez que le fait de définir un certificat comme actif peut nécessiter le rétablissement de la confiance, puis choisissez Rendre actif.

Étape 4 : Supprimez l'ancien certificat.

Suivez la procédure ci-dessous pour terminer le processus de rotation des certificats pour votre demande. Vous ne pouvez supprimer qu'un certificat dont l'état est inactif.

1. Ouvrez la console IAM Identity Center.
2. Choisissez Applications.
3. Dans la liste des applications, sélectionnez votre application.
4. Sur la page des détails de l'application, sélectionnez l'onglet Configuration. Sous les métadonnées du centre d'identité IAM, sélectionnez Gérer le certificat.
5. Sur la page du certificat IAM Identity Center, sélectionnez le certificat que vous souhaitez supprimer. Choisissez Actions, puis Delete (Supprimer).
6. Dans la boîte de dialogue Supprimer le certificat, choisissez Supprimer.

Indicateurs du statut d'expiration des certificats

Sur la page Applications, dans les propriétés d'une application, vous remarquerez peut-être des icônes d'indicateur d'état colorées. Ces icônes apparaissent dans la colonne Expire le jour à côté de chaque certificat de la liste. Ce qui suit décrit les critères utilisés par IAM Identity Center pour déterminer quelle icône est affichée pour chaque certificat.

- Rouge — Indique qu'un certificat est actuellement expiré.
- Jaune — Indique qu'un certificat expirera dans 90 jours ou moins.
- Vert — Indique qu'un certificat est actuellement valide et qu'il le restera pendant au moins 90 jours supplémentaires.

Pour vérifier l'état actuel d'un certificat

1. Ouvrez la console IAM Identity Center.
2. Choisissez Applications.
3. Dans la liste des applications, vérifiez le statut des certificats de la liste, comme indiqué dans la colonne Expire le.

Configuration des propriétés de l'application dans la console IAM Identity Center

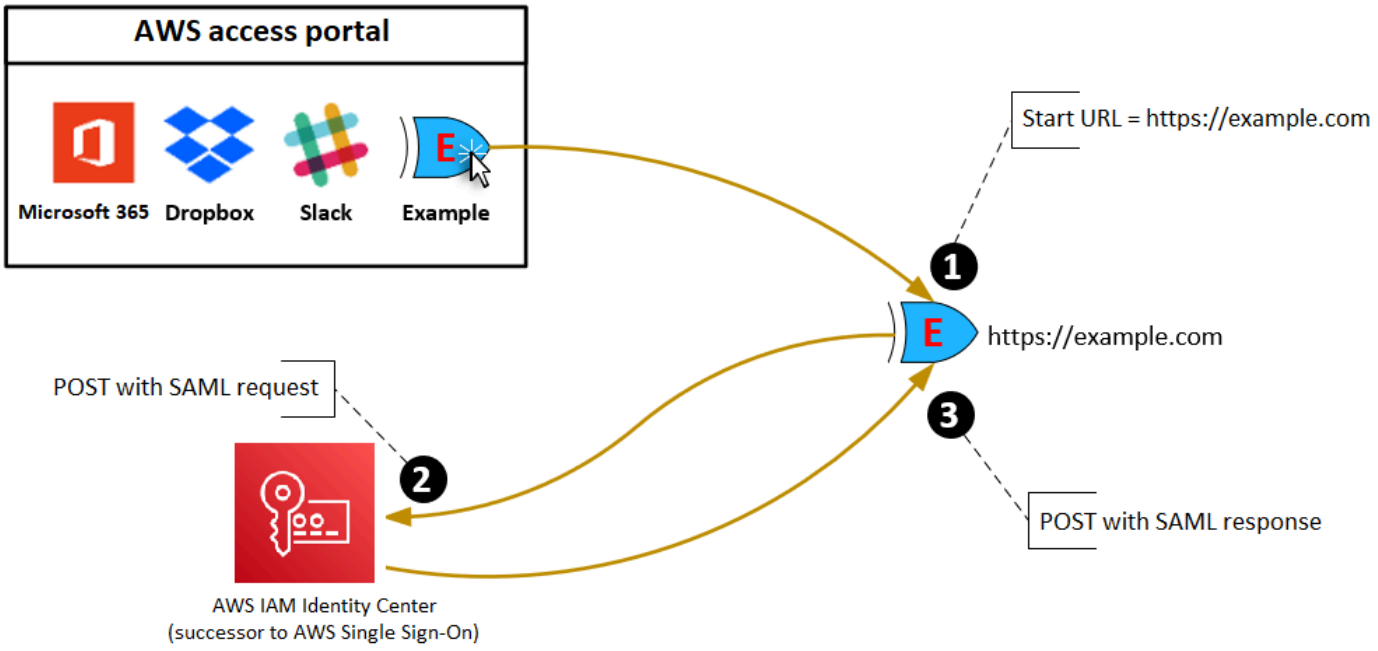
Dans IAM Identity Center, vous pouvez personnaliser l'expérience utilisateur en configurant l'URL de démarrage de l'application, l'état du relais et la durée de session.

URL de démarrage de l'application

Vous utilisez une URL de lancement d'application pour démarrer le processus de fédération avec votre application. L'utilisation typique concerne une application qui prend uniquement en charge la liaison initiée par le fournisseur de services (SP).

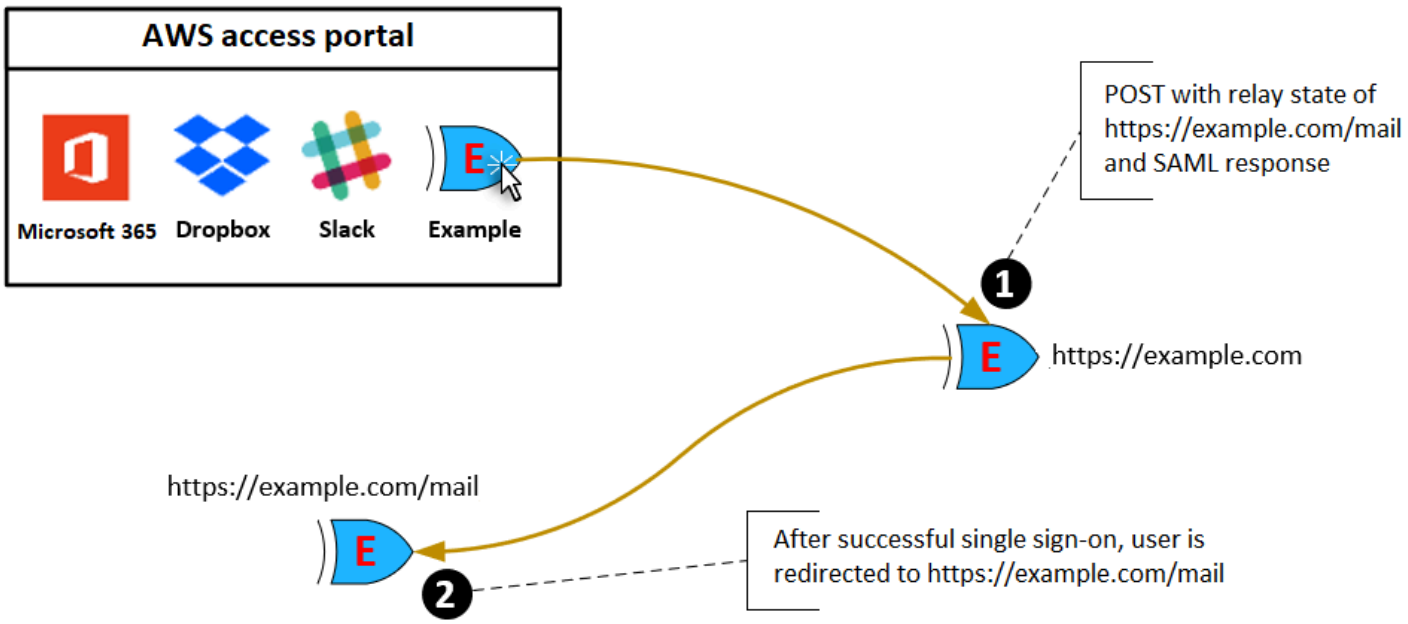
Les étapes et le schéma suivants illustrent le flux de travail d'authentification par URL de démarrage de l'application lorsqu'un utilisateur choisit une application dans le portail AWS d'accès :

1. Le navigateur de l'utilisateur redirige la demande d'authentification à l'aide de la valeur de l'URL de lancement d'application (ici https://example.com).
2. L'application envoie un `HTML POST` identifiant `SAMLRequest` à IAM Identity Center.
3. IAM Identity Center envoie ensuite un message `HTML POST` avec un `SAMLResponse` retour à l'application.



État du relais

Pendant le processus d'authentification de la fédération, l'état de relais redirige les utilisateurs au sein de l'application. Pour SAML 2.0, cette valeur est transmise, sans modification, à l'application. Une fois les propriétés de l'application configurées, IAM Identity Center envoie la valeur de l'état du relais avec une réponse SAML à l'application.



Durée de la session

La durée de session est la durée pendant laquelle une session utilisateur de l'application est valide. Pour SAML 2.0, cela est utilisé pour définir la `SessionNotOnOrAfter` date de l'élément de l'assertion SAML. `saml2:AuthNStatement`

La durée de session peut être interprétée par les applications de l'une des manières suivantes :

- Les applications peuvent l'utiliser pour déterminer la durée maximale autorisée pour la session de l'utilisateur. Les applications peuvent générer une session utilisateur d'une durée plus courte. Cela peut se produire lorsque l'application prend uniquement en charge les sessions utilisateur avec une durée plus courte que la durée de session configurée.
- Les applications peuvent l'utiliser comme durée exacte et ne pas permettre aux administrateurs de configurer la valeur. Cela peut se produire lorsque l'application prend uniquement en charge une durée de session spécifique.

Pour plus d'informations sur la façon dont la durée de la session est utilisée, consultez la documentation de votre application spécifique.

Attribuer un accès utilisateur aux applications dans la console IAM Identity Center

Vous pouvez attribuer aux utilisateurs un accès par authentification unique aux applications SAML 2.0 du catalogue d'applications ou aux applications SAML 2.0 personnalisées.

Considérations relatives aux tâches de groupe :

- Attribuez l'accès directement aux groupes. Pour simplifier l'administration des autorisations d'accès, nous vous recommandons d'attribuer l'accès directement à des groupes plutôt qu'à des utilisateurs individuels. Avec les groupes, vous pouvez accorder ou refuser des autorisations à des groupes d'utilisateurs, au lieu d'appliquer ces autorisations à chaque individu. Si un utilisateur est transféré dans une autre organisation, il vous suffit de le déplacer vers un autre groupe. L'utilisateur reçoit alors automatiquement les autorisations nécessaires à la nouvelle organisation.
- Les groupes imbriqués ne sont pas pris en charge. Lors de l'attribution d'un accès utilisateur aux applications, IAM Identity Center ne prend pas en charge l'ajout d'utilisateurs à des groupes imbriqués. Si un utilisateur est ajouté à un groupe imbriqué, il peut recevoir un message « Vous

n'avez aucune application » lors de la connexion. Les attributions doivent être effectuées par rapport au groupe immédiat dont l'utilisateur est membre.

Pour attribuer un accès aux applications à un utilisateur ou à un groupe

> **Important**
>
> Pour les applications AWS gérées, vous devez ajouter des utilisateurs directement depuis les consoles d'applications concernées ou via les API.

1. Ouvrez la console IAM Identity Center.

   > **Note**
   >
   > Si vous gérez des utilisateurs dans AWS Managed Microsoft AD, assurez-vous que la console IAM Identity Center utilise la AWS région dans laquelle se trouve votre AWS Managed Microsoft AD annuaire avant de passer à l'étape suivante.

2. Choisissez Applications.
3. Dans la liste des applications, choisissez le nom de l'application à laquelle vous souhaitez attribuer l'accès.
4. Sur la page des détails de l'application, dans la section Utilisateurs assignés, choisissez Attribuer des utilisateurs.
5. Dans la boîte de dialogue Attribuer des utilisateurs, entrez un nom d'utilisateur ou de groupe. Vous pouvez également rechercher des utilisateurs et des groupes. Vous pouvez spécifier plusieurs utilisateurs ou groupes en sélectionnant les comptes applicables tels qu'ils apparaissent dans les résultats de recherche.
6. Choisissez Assign users (Affecter des utilisateurs).

Supprimer l'accès des utilisateurs dans la console IAM Identity Center

Utilisez cette procédure pour supprimer l'accès des utilisateurs aux applications SAML 2.0 du catalogue d'applications ou aux applications SAML 2.0 personnalisées.

Pour supprimer l'accès d'un utilisateur à une application

1. Ouvrez la console IAM Identity Center.
2. Choisissez Applications.
3. Dans la liste des applications, choisissez l'application dont vous souhaitez supprimer l'accès utilisateur.
4. Sur la page des détails de l'application, dans la section Utilisateurs assignés, sélectionnez l'utilisateur ou le groupe que vous souhaitez supprimer, puis cliquez sur le bouton Supprimer l'accès.
5. Dans la boîte de dialogue Remove access (Supprimer l'accès), vérifiez le nom de l'utilisateur ou du groupe. Choisissez ensuite Remove access (Supprimer l'accès).

Associez les attributs de votre application aux attributs d'IAM Identity Center

Certains fournisseurs de services ont besoin d'assertions SAML personnalisées pour transmettre des données supplémentaires concernant les connexions des utilisateurs. Dans ce cas, utilisez la procédure suivante pour spécifier comment les attributs utilisateur de vos applications doivent correspondre aux attributs correspondants dans IAM Identity Center.

Pour mapper les attributs d'une application à des attributs dans IAM Identity Center

1. Ouvrez la console IAM Identity Center.
2. Choisissez Applications.
3. Dans la liste des applications, choisissez l'application pour laquelle vous souhaitez mapper les attributs.
4. Sur la page des détails de l'application, sélectionnez Actions, puis sélectionnez Modifier le mappage d'attributs.
5. Choisissez Ajouter un nouveau mappage d'attributs.
6. Dans la première zone de texte, entrez l'attribut de l'application.
7. Dans la deuxième zone de texte, entrez l'attribut dans IAM Identity Center que vous souhaitez associer à l'attribut de l'application. Par exemple, vous souhaiterez peut-être mapper l'attribut de l'application **`Username`** à l'attribut **`email`** utilisateur IAM Identity Center. Pour consulter la liste des attributs utilisateur autorisés dans IAM Identity Center, consultez le tableau dansMappages d'attributs pour le répertoire AWS Managed Microsoft AD.

8. Dans la troisième colonne du tableau, choisissez le format approprié pour l'attribut dans le menu.
9. Sélectionnez Enregistrer les modifications.

Conception de la résilience et comportement régional

Le service IAM Identity Center est entièrement géré et utilise des AWS services hautement disponibles et durables, tels qu'Amazon S3 et Amazon EC2. Pour garantir la disponibilité en cas d'interruption de la zone de disponibilité, IAM Identity Center fonctionne dans plusieurs zones de disponibilité. Pour plus d'informations sur les objectifs de conception de disponibilité pour IAM Identity Center, consultez l'annexe A : Conçu pour la disponibilité de certains AWS services dans le guide du pilier de fiabilité.

Vous activez IAM Identity Center dans votre compte AWS Organizations de gestion. Cela est nécessaire pour qu'IAM Identity Center puisse provisionner, déprovisionner et mettre à jour les rôles dans tous vos domaines. Comptes AWS Lorsque vous activez IAM Identity Center, celui-ci est déployé sur Région AWS le site actuellement sélectionné. Si vous souhaitez effectuer un déploiement dans une région spécifiqueRégion AWS, modifiez la sélection de la région avant d'activer IAM Identity Center.

> **Note**
>
> IAM Identity Center contrôle l'accès à ses ensembles d'autorisations et à ses applications uniquement à partir de sa région principale. Nous vous recommandons de prendre en compte les risques associés au contrôle d'accès lorsque IAM Identity Center opère dans une seule région.

Bien qu'IAM Identity Center détermine l'accès depuis la région dans laquelle vous activez le service, Comptes AWS ils sont mondiaux. Cela signifie qu'une fois que les utilisateurs se sont connectés à IAM Identity Center, ils peuvent opérer dans n'importe quelle région lorsqu'ils y accèdent Comptes AWS via IAM Identity Center. La plupart des applications AWS gérées telles qu'Amazon doivent SageMaker toutefois être installées dans la même région qu'IAM Identity Center pour que les utilisateurs puissent s'authentifier et attribuer l'accès à ces applications. Pour plus d'informations sur les contraintes régionales lors de l'utilisation d'une application avec IAM Identity Center, consultez la documentation de l'application.

Vous pouvez également utiliser IAM Identity Center pour authentifier et autoriser l'accès aux applications SAML accessibles via une URL publique, quel que soit la plateforme ou le cloud sur lequel l'application est créée.

Nous vous déconseillons de l'utiliser Instances de compte d'IAM Identity Center comme moyen de mise en œuvre de la résilience, car cela crée un deuxième point de contrôle isolé qui n'est pas connecté à l'instance de votre organisation.

Configurez un accès d'urgence au AWS Management Console

IAM Identity Center est construit à partir d'une AWS infrastructure à haute disponibilité et utilise une architecture de zone de disponibilité pour éliminer les points de défaillance uniques. Pour une couche de protection supplémentaire dans le cas peu probable d'un IAM Identity Center ou d'une Région AWS interruption, nous vous recommandons de configurer une configuration que vous pouvez utiliser pour fournir un accès temporaire auAWS Management Console.

Table des matières

Présentation

AWS vous permet d'effectuer les opérations suivantes :

- Connectez votre IdP tiers à IAM Identity Center.
- Connectez votre IdP tiers à un individu en Comptes AWS utilisant la fédération basée sur SAML 2.0.

Si vous utilisez IAM Identity Center, vous pouvez utiliser ces fonctionnalités pour créer la configuration d'accès d'urgence décrite dans les sections suivantes. Cette configuration vous permet d'utiliser IAM Identity Center comme mécanisme d'Compte AWSaccès. Si le centre d'identité IAM

est perturbé, les utilisateurs de vos opérations d'urgence peuvent se connecter à la fédération par le AWS Management Console biais de la fédération directe, en utilisant les mêmes informations d'identification que celles qu'ils utilisent pour accéder à leurs comptes. Cette configuration fonctionne lorsque le centre d'identité IAM n'est pas disponible, mais que le plan de données IAM et votre fournisseur d'identité externe (IdP) sont disponibles.

> **Important**
>
> Nous vous recommandons de déployer cette configuration avant qu'une interruption ne survienne, car vous ne pouvez pas créer la configuration si votre accès pour créer les rôles IAM requis est également perturbé. Testez également cette configuration régulièrement pour vous assurer que votre équipe comprend ce qu'elle doit faire en cas d'interruption d'IAM Identity Center.

Résumé de la configuration des accès d'urgence

Pour configurer l'accès d'urgence, vous devez effectuer les tâches suivantes :

1. Créez un compte des opérations d'urgence dans votre organisation dans AWS Organizations.
2. Connectez votre IdP au compte des opérations d'urgence à l'aide de la fédération basée sur SAML 2.0.
3. Dans le compte des opérations d'urgence, créez un rôle pour la fédération des fournisseurs d'identité tiers. Créez également un rôle d'opérations d'urgence dans chacun de vos comptes de charge de travail, avec les autorisations requises.
4. Déléguez l'accès à vos comptes de charge de travail pour le rôle IAM que vous avez créé dans le compte des opérations d'urgence. Pour autoriser l'accès à votre compte d'opérations d'urgence, créez un groupe d'opérations d'urgence dans votre IdP, sans aucun membre.
5. Permettez au groupe des opérations d'urgence de votre IdP d'utiliser le rôle des opérations d'urgence en créant une règle dans votre IdP qui autorise l'accès fédéré SAML 2.0 au. AWS Management Console

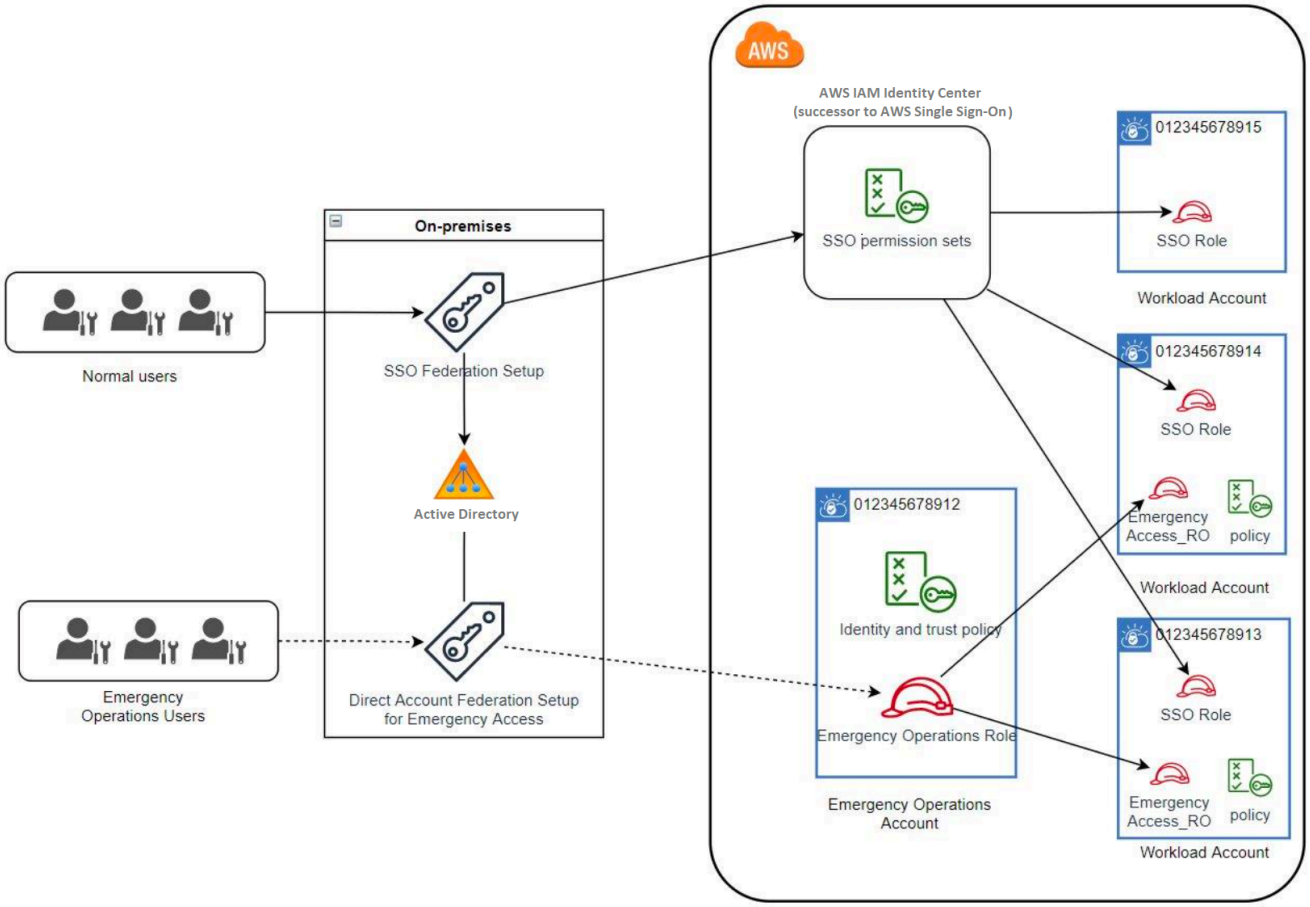
Pendant les opérations normales, personne n'a accès au compte des opérations d'urgence car le groupe des opérations d'urgence de votre IdP ne compte aucun membre. En cas d'interruption du centre d'identité IAM, utilisez votre IdP pour ajouter des utilisateurs de confiance au groupe des opérations d'urgence de votre IdP. Ces utilisateurs peuvent ensuite se connecter à votre IdP, accéder

au et assumer le AWS Management Console rôle des opérations d'urgence dans le compte des opérations d'urgence. À partir de là, ces utilisateurs peuvent passer au rôle d'accès d'urgence dans vos comptes de charge de travail où ils doivent effectuer des opérations.

Comment concevoir vos rôles opérationnels critiques

Avec cette conception, vous configurez un système unique Compte AWS dans lequel vous fédérez via IAM, afin que les utilisateurs puissent assumer des rôles opérationnels critiques. Les rôles liés aux opérations critiques sont régis par une politique de confiance qui permet aux utilisateurs d'assumer un rôle correspondant dans vos comptes de charge de travail. Les rôles des comptes de charge de travail fournissent les autorisations dont les utilisateurs ont besoin pour effectuer des tâches essentielles.

Le schéma suivant fournit une vue d'ensemble de la conception.



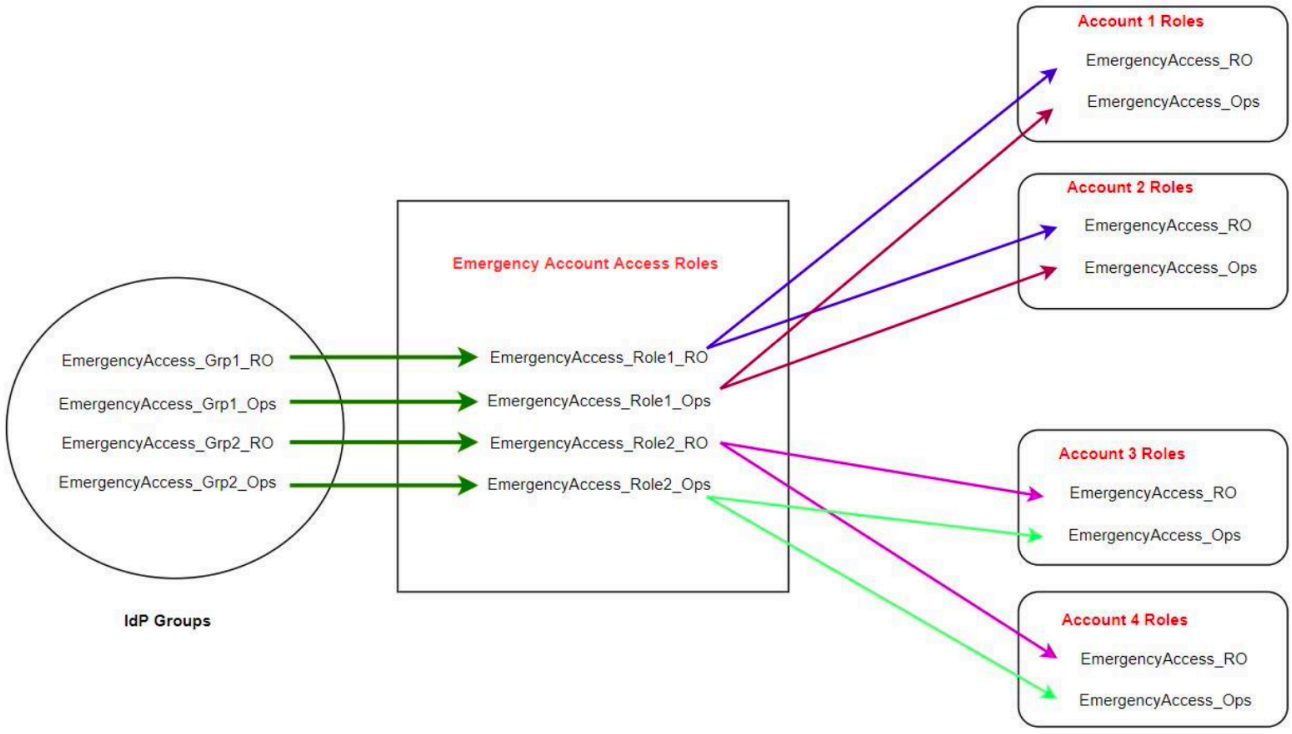
Comment planifier votre modèle d'accès

Avant de configurer l'accès d'urgence, créez un plan de fonctionnement du modèle d'accès. Utilisez le processus suivant pour créer ce plan.

1. Identifiez les Comptes AWS endroits où l'accès des opérateurs d'urgence est essentiel lors d'une interruption du IAM Identity Center. Par exemple, vos comptes de production sont probablement essentiels, mais vos comptes de développement et de test ne le sont peut-être pas.
2. Pour cette collection de comptes, identifiez les rôles critiques spécifiques dont vous avez besoin dans vos comptes. Sur l'ensemble de ces comptes, définissez de manière cohérente ce que les rôles peuvent faire. Cela simplifie le travail dans votre compte d'accès d'urgence où vous pouvez créer des rôles entre comptes. Nous vous recommandons de commencer par deux rôles distincts dans ces comptes : Read Only (RO) et Operations (Ops). Si nécessaire, vous pouvez créer d'autres rôles et les associer à un groupe plus distinct d'utilisateurs d'accès d'urgence dans votre configuration.
3. Identifiez et créez des groupes d'accès d'urgence dans votre IdP. Les membres du groupe sont les utilisateurs auxquels vous déléguez l'accès aux rôles d'accès d'urgence.
4. Définissez les rôles que ces groupes peuvent assumer dans le compte d'accès d'urgence. Pour ce faire, définissez des règles dans votre IdP qui génèrent des revendications répertoriant les rôles auxquels le groupe peut accéder. Ces groupes peuvent ensuite assumer vos rôles de lecture seule ou d'opérations dans le compte d'accès d'urgence. À partir de ces rôles, ils peuvent assumer les rôles correspondants dans vos comptes de charge de travail.

Comment concevoir un mappage des rôles, des comptes et des groupes en cas d'urgence

Le schéma suivant montre comment mapper vos groupes d'accès d'urgence aux rôles de votre compte d'accès d'urgence. Le diagramme montre également les relations de confiance entre comptes qui permettent aux rôles d'accès d'urgence d'accéder aux rôles correspondants dans vos comptes de charge de travail. Nous recommandons que la conception de votre plan d'urgence utilise ces mappages comme point de départ.



Comment créer votre configuration d'accès d'urgence

Utilisez le tableau de mappage suivant pour créer votre configuration d'accès d'urgence. Ce tableau reflète un plan qui inclut deux rôles dans les comptes de charge de travail : Read Only (RO) et Operations (Ops), avec les politiques de confiance et les politiques d'autorisation correspondantes. Les politiques de confiance permettent aux rôles des comptes d'accès d'urgence d'accéder aux rôles des comptes de charge de travail individuels. Les rôles individuels du compte de charge de travail sont également soumis à des politiques d'autorisation concernant ce que le rôle peut faire dans le compte. Les politiques d'autorisation peuvent être des politiques AWS gérées ou des politiques gérées par le client.

Compte	Rôles à créer	Politique d'approbation	Politique d'autorisations
Compte 1	Emergency Access_RO	Emergency Access_Role1_RO	arn:aws:iam::aws:policy/ReadOnlyAccess

Compte	Rôles à créer	Politique d'approbation	Politique d'autorisations
Compte 1	Emergency Access_Ops	Emergency Access_Role1_Ops	arn:aws:iam::aws:policy/job-function/SystemAdministrator
Compte 2	Emergency Access_RO	Emergency Access_Role2_RO	arn:aws:iam : :aws:policy/ReadOnlyAccess
Compte 2	Emergency Access_Ops	Emergency Access_Role2_Ops	arn:aws:iam::aws:policy/job-function/SystemAdministrator
Compte d'accès d'urgence	Emergency Access_Role1_RO Emergency Access_Role1_Ops Emergency Access_Role2_RO Emergency Access_Role2_Ops	IdP	AssumeRole pour le rôle, la ressource dans le compte

Dans ce plan de mappage, le compte d'accès d'urgence contient deux rôles en lecture seule et deux rôles opérationnels. Ces rôles font confiance à votre IdP pour authentifier et autoriser les groupes que vous avez sélectionnés à accéder aux rôles en transmettant les noms des rôles dans des assertions. Il existe des rôles de lecture seule et d'exploitation correspondants dans le compte de charge de travail 1 et le compte 2. Pour le compte de charge de travail 1, le `EmergencyAccess_RO` rôle fait confiance au `EmergencyAccess_Role1_RO` rôle qui réside dans le compte d'accès d'urgence. Le tableau indique des modèles de confiance similaires entre les rôles de lecture seule et d'exploitation du compte de charge de travail et les rôles d'accès d'urgence correspondants.

Tâches de préparation aux urgences

Pour préparer la configuration de votre accès d'urgence, nous vous recommandons d'effectuer les tâches suivantes avant qu'une urgence ne se produise.

1. Configurez une application de fédération IAM directe dans votre IdP. Pour plus d'informations, consultez Configuration unique d'une application de fédération IAM directe dans Okta.
2. Créez une connexion IdP dans le compte d'accès d'urgence accessible pendant l'événement.
3. Créez des rôles d'accès d'urgence dans les comptes d'accès d'urgence, comme décrit dans le tableau de mappage ci-dessus.
4. Créez des rôles opérationnels temporaires avec des politiques de confiance et d'autorisation dans chacun des comptes de charge de travail.
5. Créez des groupes d'opérations temporaires dans votre IdP. Les noms des groupes dépendront des noms des rôles des opérations temporaires.
6. Testez la fédération IAM directe.
7. Désactivez l'application de fédération IdP dans votre IdP pour empêcher une utilisation régulière.

Processus de basculement d'urgence

Lorsqu'une instance IAM Identity Center n'est pas disponible et que vous déterminez que vous devez fournir un accès d'urgence à la console AWS de gestion, nous recommandons le processus de basculement suivant.

1. L'administrateur de l'IdP active l'application de fédération IAM directe dans votre IdP.
2. Les utilisateurs demandent l'accès au groupe des opérations temporaires par le biais de votre mécanisme existant, tel qu'une demande par e-mail, un canal Slack ou une autre forme de communication.
3. Les utilisateurs que vous ajoutez à vos groupes d'accès d'urgence se connectent à l'IdP, sélectionnent le compte d'accès d'urgence, puis les utilisateurs choisissent un rôle à utiliser dans le compte d'accès d'urgence. À partir de ces rôles, ils peuvent assumer des rôles dans les comptes de charge de travail correspondants bénéficiant d'une confiance croisée avec le rôle de compte d'urgence.

Retour aux activités normales

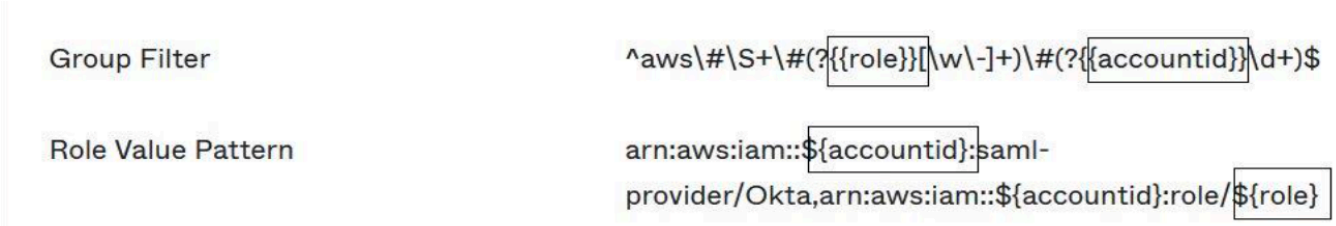
Consultez le AWSHealth Dashboard pour confirmer le moment où l'état du service IAM Identity Center est rétabli. Pour revenir à un fonctionnement normal, effectuez les opérations suivantes.

1. Une fois que l'icône d'état du service IAM Identity Center indique que le service est en bon état, connectez-vous à IAM Identity Center.
2. Si vous parvenez à vous connecter à IAM Identity Center, informez les utilisateurs d'accès d'urgence qu'IAM Identity Center est disponible. Demandez à ces utilisateurs de se déconnecter et d'utiliser le portail AWS d'accès pour se reconnecter à IAM Identity Center.
3. Une fois que tous les utilisateurs d'accès d'urgence se sont déconnectés, dans l'IdP, désactivez l'application de fédération IdP. Nous vous recommandons d'effectuer cette tâche en dehors des heures de travail.
4. Supprimez tous les utilisateurs du groupe d'accès d'urgence dans l'IdP.

Votre infrastructure de rôles d'accès d'urgence reste en place en tant que plan d'accès de secours, mais elle est désormais désactivée.

Configuration unique d'une application de fédération IAM directe dans Okta

1. Connectez-vous à votre Okta compte en tant qu'utilisateur disposant d'autorisations administratives.
2. Dans la Okta console d'administration, sous Applications, sélectionnez Applications.
3. Choisissez Parcourir le catalogue d'applications. Recherchez et choisissez AWSAccount Federation. Choisissez ensuite Ajouter une intégration.
4. Configurez la fédération IAM directe avec AWS en suivant les étapes décrites dans Comment configurer SAML 2.0 pour la fédération de AWS comptes.
5. Dans l'onglet Options de connexion, sélectionnez SAML 2.0 et entrez les paramètres du filtre de groupe et du modèle de valeur des rôles. Le nom du groupe pour l'annuaire des utilisateurs dépend du filtre que vous configurez.



Dans la figure ci-dessus, la `role` variable concerne le rôle des opérations d'urgence dans votre compte d'accès d'urgence. Par exemple, si vous créez le `EmergencyAccess_Role1_RO` rôle (comme décrit dans le tableau de mappage) dans Compte AWS`123456789012`, et si votre paramètre de filtre de groupe est configuré comme indiqué dans la figure ci-dessus, le nom de votre groupe doit être`aws#EmergencyAccess_Role1_RO#123456789012`.

6. Dans votre répertoire (par exemple, votre répertoire dans Active Directory), créez le groupe d'accès d'urgence et attribuez un nom au répertoire (par exemple,`aws#EmergencyAccess_Role1_RO#123456789012`). Affectez vos utilisateurs à ce groupe en utilisant votre mécanisme de provisionnement existant.
7. Dans le compte d'accès d'urgence, configurez une politique de confiance personnalisée qui fournit les autorisations requises pour que le rôle d'accès d'urgence soit assumé lors d'une interruption. Vous trouverez ci-dessous un exemple de déclaration pour une politique de confiance personnalisée attachée au `EmergencyAccess_Role1_RO` rôle. Pour une illustration, voir le compte d'urgence dans le schéma ci-dessousComment concevoir un mappage des rôles, des comptes et des groupes en cas d'urgence.

```
{
    "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. Voici un exemple de déclaration pour une politique d'autorisation attachée au `EmergencyAccess_Role1_R0` rôle. Pour une illustration, voir le compte d'urgence dans le schéma ci-dessousComment concevoir un mappage des rôles, des comptes et des groupes en cas d'urgence.

```
{
    "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. Sur les comptes de charge de travail, configurez une politique de confiance personnalisée. Vous trouverez ci-dessous un exemple de déclaration pour une politique de confiance attachée au `EmergencyAccess_R0` rôle. Dans cet exemple, le compte `123456789012` est le compte d'accès d'urgence. Pour une illustration, voir le compte de charge de travail dans le schéma ci-dessousComment concevoir un mappage des rôles, des comptes et des groupes en cas d'urgence.

```
{
    "Version": "2012-10-17",
    "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "AWS":"arn:aws:iam::123456789012:root"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

> **Note**
>
> La plupart vous IdPs permettent de désactiver l'intégration d'une application jusqu'à ce que vous en ayez besoin. Nous vous recommandons de laisser l'application de fédération IAM directe désactivée dans votre IdP jusqu'à ce qu'elle soit requise pour un accès d'urgence.

Sécurité dans AWS IAM Identity Center

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de conformitéAWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS IAM Identity Center, consultez la section AWS Services concernés par programme de conformité.
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation d'IAM Identity Center. Les rubriques suivantes expliquent comment configurer IAM Identity Center pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser les ressources de votre IAM Identity Center.

Rubriques

Gestion des identités et des accès pour IAM Identity Center

L'accès à IAM Identity Center nécessite des informations d'identification qui AWS peuvent être utilisées pour authentifier vos demandes. Ces informations d'identification doivent être autorisées à accéder aux AWS ressources, telles qu'une application AWS gérée.

L'authentification sur le portail AWS d'accès est contrôlée par le répertoire que vous avez connecté à IAM Identity Center. Cependant, l' Comptes AWS autorisation accordée aux utilisateurs depuis le portail AWS d'accès est déterminée par deux facteurs :

1. Qui a reçu l'accès à ceux de Comptes AWS la console IAM Identity Center. Pour plus d'informations, consultez Accès par authentification unique à Comptes AWS.
2. Quel niveau d'autorisations a été accordé aux utilisateurs dans la console IAM Identity Center pour leur permettre d'y accéder de manière appropriée ? Comptes AWS Pour plus d'informations, consultez Création, gestion et suppression d'ensembles d'autorisations.

Les sections suivantes expliquent comment, en tant qu'administrateur, vous pouvez contrôler l'accès à la console IAM Identity Center ou déléguer l'accès administratif aux day-to-day tâches depuis la console IAM Identity Center.

- Authentification
- Contrôle d'accès

Authentification

Découvrez comment accéder à l' AWS aide des identités IAM.

Contrôle d'accès

Vous pouvez disposer d'informations d'identification valides pour authentifier vos demandes, mais vous ne pouvez pas créer de ressources IAM Identity Center ou y accéder sans autorisation. Par exemple, vous devez disposer des autorisations nécessaires pour créer un répertoire connecté à IAM Identity Center.

Les sections suivantes décrivent comment gérer les autorisations pour IAM Identity Center. Nous vous recommandons de lire d'abord la présentation.

- Présentation de la gestion des autorisations d'accès aux ressources de votre IAM Identity Center
- Exemples de politiques basées sur l'identité pour IAM Identity Center
- Utilisation de rôles liés à un service pour IAM Identity Center

Présentation de la gestion des autorisations d'accès aux ressources de votre IAM Identity Center

Chaque AWS ressource appartient à un Compte AWS, et les autorisations de création ou d'accès aux ressources sont régies par des politiques d'autorisation. Pour fournir un accès, un administrateur de compte peut ajouter des autorisations aux identités IAM (c'est-à-dire aux utilisateurs, aux groupes et aux rôles). Certains services (tels que AWS Lambda) prennent également en charge l'ajout d'autorisations aux ressources.

> **Note**
>
> Un administrateur de compte (ou utilisateur administrateur) est un utilisateur doté des privilèges d'administrateur. Pour plus d'informations, consultez Bonnes pratiques IAM dans le Guide de l'utilisateur IAM.

Rubriques

- Ressources et opérations de l'IAM Identity Center
- Présentation de la propriété des ressources
- Gestion de l'accès aux ressources
- Spécification des éléments de politique : actions, effets, ressources et principes
- Spécification de conditions dans une politique

Ressources et opérations de l'IAM Identity Center

Dans IAM Identity Center, les ressources principales sont les instances d'applications, les profils et les ensembles d'autorisations.

Présentation de la propriété des ressources

Le propriétaire d'une ressource est celui Compte AWS qui a créé une ressource. En d'autres termes, le propriétaire Compte AWS de la ressource est l'entité principale (le compte, un utilisateur ou un rôle

IAM) qui authentifie la demande qui crée la ressource. Les exemples suivants illustrent comment cela fonctionne :

- Si le Utilisateur racine d'un compte AWS crée une ressource IAM Identity Center, telle qu'une instance d'application ou un ensemble d'autorisations, vous Compte AWS êtes le propriétaire de cette ressource.
- Si vous créez un utilisateur dans votre AWS compte et que vous lui accordez les autorisations nécessaires pour créer des ressources IAM Identity Center, l'utilisateur peut alors créer des ressources IAM Identity Center. Cependant, votre AWS compte, auquel appartient l'utilisateur, est propriétaire des ressources.
- Si vous créez un rôle IAM dans votre AWS compte avec les autorisations nécessaires pour créer des ressources IAM Identity Center, toute personne pouvant assumer ce rôle peut créer des ressources IAM Identity Center. Vous Compte AWS, à qui appartient le rôle, êtes propriétaire des ressources de l'IAM Identity Center.

Gestion de l'accès aux ressources

Une politique d'autorisation décrit qui a accès à quoi. La section suivante explique les options disponibles pour créer des politiques d'autorisations.

> **Note**
>
> Cette section décrit l'utilisation d'IAM dans le contexte d'IAM Identity Center. Elle ne fournit pas d'informations détaillées sur le service IAM. Pour une documentation complète sur IAM, consultez la rubrique Qu'est-ce que IAM ? dans le Guide de l'utilisateur IAM. Pour plus d'informations sur la syntaxe et les descriptions des politiques IAM, consultez la Référence des politiques AWS IAM dans le Guide de l'utilisateur IAM.

Les politiques qui sont associées à une identité IAM sont appelées des politiques basées sur l'identité (politiques IAM). Les politiques qui sont attachées à une ressource sont appelées politiques basées sur la ressource. IAM Identity Center prend uniquement en charge les politiques basées sur l'identité (politiques IAM).

Rubriques

- Politiques basées sur une identité (politiques IAM)
- Politiques basées sur les ressources

Politiques basées sur une identité (politiques IAM)

Vous pouvez ajouter des autorisations aux identités IAM. Par exemple, vous pouvez effectuer les opérations suivantes :

- Associez une politique d'autorisations à un utilisateur ou à un groupe de votre compte Compte AWS : un administrateur de compte peut utiliser une politique d'autorisations associée à un utilisateur particulier pour autoriser cet utilisateur à ajouter une ressource IAM Identity Center, telle qu'une nouvelle application.
- Attacher une politique d'autorisations à un rôle (accorder des autorisations entre comptes) : vous pouvez attacher une politique d'autorisation basée sur une identité à un rôle IAM afin d'accorder des autorisations entre comptes.

  Pour plus d'informations sur l'utilisation d'IAM pour déléguer des autorisations, veuillez consulter la section Access management (français non garanti) dans le Guide de l'utilisateur IAM.

La politique d'autorisation suivante accorde des autorisations à un utilisateur lui permettant d'exécuter toutes les actions commençant par `List`. Ces actions affichent des informations sur une ressource IAM Identity Center, telle qu'une instance d'application ou un ensemble d'autorisations. Notez que le caractère générique (*) dans l'`Resource`élément indique que les actions sont autorisées pour toutes les ressources IAM Identity Center détenues par le compte.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"sso:List*",
         "Resource":"*"
      }
   ]
}
```

Pour plus d'informations sur l'utilisation de politiques basées sur l'identité avec IAM Identity Center, consultez. Exemples de politiques basées sur l'identité pour IAM Identity Center Pour plus d'informations sur les utilisateurs, les groupes, les rôles et les autorisations, consultez Identités (utilisateurs, groupes et rôles) dans le Guide de l'utilisateur IAM.

Politiques basées sur les ressources

D'autres services, tels qu'Amazon S3, prennent également en charge les politiques d'autorisation basées sur une ressource. Par exemple, vous pouvez attacher une politique à un compartiment S3 pour gérer les autorisations d'accès à ce compartiment. IAM Identity Center ne prend pas en charge les politiques basées sur les ressources.

Spécification des éléments de politique : actions, effets, ressources et principes

Pour chaque ressource IAM Identity Center (voirRessources et opérations de l'IAM Identity Center), le service définit un ensemble d'opérations d'API. Pour accorder des autorisations pour ces opérations d'API, IAM Identity Center définit un ensemble d'actions que vous pouvez spécifier dans une politique. Notez que l'exécution d'une opération d'API peut exiger des autorisations pour plusieurs actions.

Voici les éléments de base d'une politique :

- Ressource : dans une politique, vous utilisez un Amazon Resource Name (ARN) pour identifier la ressource à laquelle la politique s'applique.
- Action : vous utilisez des mots clés d'action pour identifier les opérations de ressource que vous voulez accorder ou refuser. Par exemple, l'`sso:DescribePermissionsPolicies`autorisation autorise l'utilisateur à effectuer l'`DescribePermissionsPolicies`opération IAM Identity Center.
- Effet – Vous spécifiez l'effet produit lorsque l'utilisateur demande l'action spécifique, qui peut être une autorisation ou un refus. Si vous n'accordez pas explicitement l'accès pour (autoriser) une ressource, l'accès est implicitement refusé. Vous pouvez aussi explicitement refuser l'accès à une ressource, ce que vous pouvez faire afin de vous assurer qu'un utilisateur n'y a pas accès, même si une politique différente accorde l'accès.
- Principal – dans les politiques basées sur une identité (politiques IAM), l'utilisateur auquel la politique est attachée est le principal implicite. Pour les politiques basées sur une ressource, vous spécifiez l'utilisateur, le compte, le service ou une autre entité qui doit recevoir les autorisations (s'applique uniquement aux politiques basées sur une ressource). IAM Identity Center ne prend pas en charge les politiques basées sur les ressources.

Pour en savoir plus sur la syntaxe et les descriptions des politiques IAM, consultez la Référence des politiques AWS IAM dans le Guide de l'utilisateur IAM.

Spécification de conditions dans une politique

Lorsque vous accordez des autorisations, vous pouvez utiliser le langage d'access policy pour spécifier les conditions qui doivent être remplies pour qu'une stratégie prenne effet. Par exemple, il est possible d'appliquer une politique après seulement une date spécifique. Pour plus d'informations sur la spécification de conditions dans un langage de politique, consultez Condition dans le Guide de l'utilisateur IAM.

Pour exprimer des conditions, vous utilisez des clés de condition prédéfinies. Il n'existe aucune clé de condition spécifique à IAM Identity Center. Cependant, il existe des clés de AWS condition que vous pouvez utiliser selon les besoins. Pour obtenir la liste complète des AWS clés, consultez la section Clés de condition globales disponibles dans le guide de l'utilisateur IAM.

Exemples de politiques basées sur l'identité pour IAM Identity Center

Cette rubrique fournit des exemples de politiques IAM que vous pouvez créer pour accorder aux utilisateurs et aux rôles les autorisations nécessaires à l'administration d'IAM Identity Center.

> **Important**
>
> Nous vous recommandons de consulter d'abord les rubriques d'introduction qui expliquent les concepts de base et les options disponibles pour gérer l'accès aux ressources de votre IAM Identity Center. Pour plus d'informations, consultez Présentation de la gestion des autorisations d'accès aux ressources de votre IAM Identity Center.

Les sections de cette rubrique couvrent les sujets suivants :

- Exemples de politiques personnalisées
- Autorisations requises pour utiliser la console IAM Identity Center

Exemples de politiques personnalisées

Cette section fournit des exemples de cas d'utilisation courants qui nécessitent une politique IAM personnalisée. Ces exemples de politiques sont des politiques basées sur l'identité, qui ne spécifient pas l'élément principal. En effet, avec une politique basée sur l'identité, vous ne spécifiez pas le principal qui obtient l'autorisation. Au lieu de cela, vous attachez la politique au principal. Lorsque vous associez une politique d'autorisation basée sur l'identité à un rôle IAM, le principal identifié dans la politique de confiance du rôle obtient les autorisations. Vous pouvez créer des politiques

basées sur l'identité dans IAM et les associer à des utilisateurs, des groupes et/ou des rôles. Vous pouvez également appliquer ces politiques aux utilisateurs d'IAM Identity Center lorsque vous créez un ensemble d'autorisations dans IAM Identity Center.

> **Note**
>
> Utilisez ces exemples lorsque vous créez des politiques pour votre environnement et assurez-vous de tester les cas positifs (« accès accordé ») et négatifs (« accès refusé ») avant de déployer ces politiques dans votre environnement de production. Pour plus d'informations sur le test des politiques IAM, consultez la section Tester les politiques IAM avec le simulateur de politiques IAM dans le guide de l'utilisateur IAM.

Rubriques

- Exemple 1 : Autoriser un utilisateur à consulter le centre d'identité IAM
- Exemple 2 : Autoriser un utilisateur à gérer les autorisations Comptes AWS dans IAM Identity Center
- Exemple 3 : autoriser un utilisateur à gérer des applications dans IAM Identity Center
- Exemple 4 : Autoriser un utilisateur à gérer les utilisateurs et les groupes dans votre annuaire Identity Center

Exemple 1 : Autoriser un utilisateur à consulter le centre d'identité IAM

La politique d'autorisation suivante accorde des autorisations en lecture seule à un utilisateur afin qu'il puisse consulter tous les paramètres et informations d'annuaire configurés dans IAM Identity Center.

> **Note**
>
> Cette politique n'est fournie qu'à titre d'exemple. Dans un environnement de production, nous vous recommandons d'utiliser la politique `ViewOnlyAccess` AWS gérée pour IAM Identity Center.

```
{
    "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": "*"
        }
    ]
}
```

Exemple 2 : Autoriser un utilisateur à gérer les autorisations Comptes AWS dans IAM Identity Center

La politique d'autorisation suivante accorde des autorisations permettant à un utilisateur de créer, de gérer et de déployer des ensembles d'autorisations pour votre Comptes AWS.

```
{
    "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**
>
> Les autorisations supplémentaires répertoriées sous `"Sid": "IAMListPermissions"` les `"Sid": "AccessToSSOProvisiondRoles"` sections et sont requises uniquement pour permettre à l'utilisateur de créer des attributions dans le compte AWS Organizations de gestion. Dans certains cas, vous devrez peut-être également ajouter des éléments `iam:UpdateSAMLProvider` à ces sections.

Exemple 3 : autoriser un utilisateur à gérer des applications dans IAM Identity Center

La politique d'autorisation suivante accorde des autorisations permettant à un utilisateur de visualiser et de configurer des applications dans IAM Identity Center, y compris des applications SaaS préintégrées issues du catalogue IAM Identity Center.

> **Note**
>
> L'`sso:AssociateProfile`opération utilisée dans l'exemple de politique suivant est requise pour la gestion des affectations d'utilisateurs et de groupes aux applications. Il permet également à un utilisateur d'attribuer des utilisateurs et des groupes à Comptes AWS l'aide des ensembles d'autorisations existants. Si un utilisateur doit gérer l' Compte AWS accès au sein d'IAM Identity Center et qu'il a besoin des autorisations nécessaires pour gérer les ensembles d'autorisations, consultezExemple 2 : Autoriser un utilisateur à gérer les autorisations Comptes AWS dans IAM Identity Center.

Depuis octobre 2020, bon nombre de ces opérations ne sont disponibles que via la AWS console. Cet exemple de politique inclut des actions de « lecture » telles que list, get et search, qui sont pertinentes pour le fonctionnement sans erreur de la console dans ce cas.

```
{
    "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": "*"
        }
    ]
}
```

Exemple 4 : Autoriser un utilisateur à gérer les utilisateurs et les groupes dans votre annuaire Identity Center

La politique d'autorisation suivante accorde des autorisations permettant à un utilisateur de créer, d'afficher, de modifier et de supprimer des utilisateurs et des groupes dans IAM Identity Center.

Dans certains cas, les modifications directes apportées aux utilisateurs et aux groupes dans IAM Identity Center sont limitées. Par exemple, lorsqu'Active Directory ou un fournisseur d'identité externe avec le provisionnement automatique activé est sélectionné comme source d'identité.

```
{
    "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": "*"
        }
    ]
}
```

Autorisations requises pour utiliser la console IAM Identity Center

Pour qu'un utilisateur puisse utiliser la console IAM Identity Center sans erreur, des autorisations supplémentaires sont nécessaires. Si une politique IAM plus restrictive que les autorisations minimales requises a été créée, la console ne fonctionnera pas comme prévu pour les utilisateurs dotés de cette politique. L'exemple suivant répertorie l'ensemble des autorisations qui peuvent être nécessaires pour garantir un fonctionnement sans erreur dans la console IAM Identity Center.

```
{
    "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 politiques gérées pour IAM Identity Center

La création de politiques gérées par les clients IAM qui fournissent à votre équipe uniquement les autorisations dont elle a besoin demande du temps et de l'expertise. Pour démarrer rapidement, vous pouvez utiliser des politiques AWS gérées. Ces politiques couvrent des cas d'utilisation courants et sont disponibles dans votre Compte AWS. Pour plus d'informations sur les politiques gérées AWS , consultez Politiques gérées AWS dans le Guide de l'utilisateur IAM.

AWS les services maintiennent et mettent à jour les politiques AWS gérées. Vous ne pouvez pas modifier les autorisations dans les politiques AWS gérées. Les services ajoutent occasionnellement des autorisations à une politique gérée par AWS pour prendre en charge de nouvelles fonctionnalités. Ce type de mise à jour affecte toutes les identités (utilisateurs, groupes et rôles) auxquelles la politique est attachée. Les services sont très susceptibles de mettre à jour une politique gérée par AWS quand une nouvelle fonctionnalité est lancée ou quand de nouvelles opérations sont disponibles. Les services ne suppriment pas les autorisations d'une politique AWS gérée. Les mises à jour des politiques n'endommageront donc pas vos autorisations existantes.

En outre, AWS prend en charge les politiques gérées pour les fonctions professionnelles qui couvrent plusieurs services. Par exemple, la politique ReadOnlyAccess AWS gérée fournit un accès en lecture seule à tous les AWS services et ressources. Lorsqu'un service lance une nouvelle fonctionnalité, il AWS ajoute des autorisations en lecture seule pour les nouvelles opérations et ressources. Pour

obtenir la liste des politiques de fonctions professionnelles et leurs descriptions, consultez la page politiques gérées par AWS pour les fonctions de tâche dans le Guide de l'utilisateur IAM.

De nouvelles actions vous permettant de répertorier et de supprimer des sessions utilisateur sont disponibles dans le nouvel espace de nomsidentitystore-auth. Toutes les autorisations supplémentaires pour les actions dans cet espace de noms seront mises à jour sur cette page. Lorsque vous créez vos politiques IAM personnalisées, évitez d'utiliser * after, identitystore-auth car cela s'applique à toutes les actions existant dans l'espace de noms aujourd'hui ou à l'avenir.

AWS politique gérée : AWSSSOMasterAccountAdministrator

La AWSSSOMasterAccountAdministrator politique fournit les mesures administratives requises aux directeurs d'école. La politique est destinée aux directeurs qui jouent le rôle d' AWS IAM Identity Center administrateur. Au fil du temps, la liste des actions fournies sera mise à jour pour correspondre aux fonctionnalités existantes d'IAM Identity Center et aux actions requises en tant qu'administrateur.

Vous pouvez associer la politique AWSSSOMasterAccountAdministrator à vos identités IAM. Lorsque vous associez la AWSSSOMasterAccountAdministrator politique à une identité, vous accordez AWS IAM Identity Center des autorisations administratives. Les principaux détenteurs de cette politique peuvent accéder à IAM Identity Center depuis le compte de AWS Organizations gestion et tous les comptes des membres. Ce principal peut gérer entièrement toutes les opérations du centre d'identité IAM, y compris la possibilité de créer une instance d'IAM Identity Center, des utilisateurs, des ensembles d'autorisations et des attributions. Le principal peut également instancier ces attributions dans les comptes des membres de l' AWS organisation et établir des connexions entre les annuaires AWS Directory Service gérés et IAM Identity Center. Au fur et à mesure que de nouvelles fonctionnalités administratives seront publiées, ces autorisations seront automatiquement accordées à l'administrateur du compte.

Regroupements d'autorisations

Cette politique est groupée en instructions basées sur le jeu d'autorisations fourni.

- AWSSSOMasterAccountAdministrator— Permet à IAM Identity Center de transmettre le rôle de service nommé AWSServiceRoleforSSO à IAM Identity Center afin qu'il puisse ultérieurement assumer le rôle et effectuer des actions en son nom. Cela est nécessaire lorsque la personne ou l'application tente d'activer IAM Identity Center. Pour plus d'informations, consultez Gérez l'accès à Comptes AWS.

- `AWSSSOMemberAccountAdministrator`— Permet à IAM Identity Center d'effectuer des actions d'administrateur de compte dans un environnement multi-comptes AWS . Pour plus d'informations, consultez AWS politique gérée : AWSSSOMemberAccountAdministrator.
- `AWSSSOManageDelegatedAdministrator`— Permet à IAM Identity Center d'enregistrer et de désenregistrer un administrateur délégué pour votre organisation.

Pour consulter les autorisations associées à cette politique, reportez-vous AWSSSOMasterAccountAdministratorà la section AWS Managed Policy Reference.

Informations supplémentaires sur cette politique

Lorsque IAM Identity Center est activé pour la première fois, le service IAM Identity Center crée un rôle lié au service dans le compte de AWS Organizations gestion (ancien compte principal) afin que IAM Identity Center puisse gérer les ressources de votre compte. Les actions requises sont `iam:CreateServiceLinkedRole` et`iam:PassRole`, comme indiqué dans les extraits suivants.

```
{
   "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 politique gérée : AWSSSOMemberAccountAdministrator

La `AWSSSOMemberAccountAdministrator` politique fournit les mesures administratives requises aux directeurs d'école. La politique est destinée aux directeurs qui jouent le rôle d'administrateur du centre d'identité IAM. Au fil du temps, la liste des actions fournies sera mise à jour pour correspondre aux fonctionnalités existantes d'IAM Identity Center et aux actions requises en tant qu'administrateur.

Vous pouvez associer la politique `AWSSSOMemberAccountAdministrator` à vos identités IAM. Lorsque vous associez la `AWSSSOMemberAccountAdministrator` politique à une identité, vous accordez AWS IAM Identity Center des autorisations administratives. Les principaux détenteurs de cette politique peuvent accéder à IAM Identity Center depuis le compte de AWS Organizations gestion et tous les comptes des membres. Ce principal peut gérer entièrement toutes les opérations de l'IAM Identity Center, y compris la possibilité de créer des utilisateurs, des ensembles d'autorisations et des attributions. Le principal peut également instancier ces attributions dans les comptes des membres de l' AWS organisation et établir des connexions entre les annuaires AWS Directory Service gérés et IAM Identity Center. À mesure que de nouvelles fonctionnalités administratives sont publiées, ces autorisations sont automatiquement accordées à l'administrateur du compte.

Pour consulter les autorisations associées à cette politique, reportez-vous AWSSSOMemberAccountAdministratorà la section AWS Managed Policy Reference.

Informations supplémentaires sur cette politique

Les administrateurs d'IAM Identity Center gèrent les utilisateurs, les groupes et les mots de passe dans leur répertoire Identity Center (répertoire SSO). Le rôle d'administrateur du compte inclut des autorisations pour les actions suivantes :

- `"sso:*"`
- `"sso-directory:*"`

Les administrateurs d'IAM Identity Center ont besoin d'autorisations limitées pour effectuer les AWS Directory Service actions suivantes afin d'effectuer les tâches quotidiennes.

- "ds:DescribeTrusts"
- "ds:UnauthorizeApplication"
- "ds:DescribeDirectories"
- "ds:AuthorizeApplication"
- “ds:CreateAlias”

Ces autorisations permettent aux administrateurs d'IAM Identity Center d'identifier les annuaires existants et de gérer les applications afin qu'elles puissent être configurées pour être utilisées avec IAM Identity Center. Pour plus d'informations sur chacune de ces actions, consultez Autorisations AWS Directory Service d'API : référence des actions, des ressources et des conditions.

IAM Identity Center utilise des politiques IAM pour accorder des autorisations aux utilisateurs d'IAM Identity Center. Les administrateurs d'IAM Identity Center créent des ensembles d'autorisations et y associent des politiques. L'administrateur du centre d'identité IAM doit être autorisé à répertorier les politiques existantes afin de pouvoir choisir les politiques à utiliser avec l'ensemble d'autorisations qu'il crée ou met à jour. Pour définir des autorisations sécurisées et fonctionnelles, l'administrateur du centre d'identité IAM doit disposer des autorisations nécessaires pour exécuter la validation de la politique d'IAM Access Analyzer.

- "iam:ListPolicies"
- "access-analyzer:ValidatePolicy"

Les administrateurs d'IAM Identity Center ont besoin d'un accès limité aux AWS Organizations actions suivantes pour effectuer leurs tâches quotidiennes :

- "organizations:EnableAWSServiceAccess"
- "organizations:ListRoots"
- "organizations:ListAccounts"
- "organizations:ListOrganizationalUnitsForParent"
- "organizations:ListAccountsForParent"
- "organizations:DescribeOrganization"
- "organizations:ListChildren"
- "organizations:DescribeAccount"
- "organizations:ListParents"

- `"organizations:ListDelegatedAdministrators"`
- `"organizations:RegisterDelegatedAdministrator"`
- `"organizations:DeregisterDelegatedAdministrator"`

Ces autorisations permettent aux administrateurs d'IAM Identity Center de travailler avec les ressources de l'organisation (comptes) pour les tâches administratives de base d'IAM Identity Center, telles que les suivantes :

- Identifier le compte de gestion appartenant à l'organisation
- Identifier les comptes des membres appartenant à l'organisation
- Activation AWS de l'accès aux services pour les comptes
- Configuration et gestion d'un administrateur délégué

Pour plus d'informations sur l'utilisation d'un administrateur délégué avec IAM Identity Center, consultezAdministration déléguée. Pour plus d'informations sur la manière dont ces autorisations sont utilisées AWS Organizations, consultez la section Utilisation AWS Organizations avec d'autres AWS services.

AWS politique gérée : AWSSSODirectoryAdministrator

Vous pouvez associer la politique `AWSSSODirectoryAdministrator` à vos identités IAM.

Cette politique accorde des autorisations administratives aux utilisateurs et aux groupes d'IAM Identity Center. Les responsables auxquels cette politique est attachée peuvent apporter des mises à jour aux utilisateurs et aux groupes IAM Identity Center.

Pour consulter les autorisations associées à cette politique, reportez-vous AWSSSODirectoryAdministratorà la section AWS Managed Policy Reference.

AWS politique gérée : AWSSSOReadOnly

Vous pouvez associer la politique `AWSSSOReadOnly` à vos identités IAM.

Cette politique accorde des autorisations en lecture seule qui permettent aux utilisateurs de consulter les informations dans IAM Identity Center. Les principaux auxquels cette politique est attachée ne peuvent pas voir directement les utilisateurs ou les groupes de l'IAM Identity Center. Les principaux auxquels cette politique est attachée ne peuvent effectuer aucune mise à jour dans IAM Identity

Center. Par exemple, les principaux disposant de ces autorisations peuvent consulter les paramètres du centre d'identité IAM, mais ne peuvent modifier aucune des valeurs des paramètres.

Pour consulter les autorisations associées à cette politique, reportez-vous AWSSSOReadOnlyà la section AWS Managed Policy Reference.

AWS politique gérée : AWSSSODirectoryReadOnly

Vous pouvez associer la politique `AWSSSODirectoryReadOnly` à vos identités IAM.

Cette politique accorde des autorisations en lecture seule qui permettent aux utilisateurs de visualiser les utilisateurs et les groupes dans IAM Identity Center. Les responsables auxquels cette politique est attachée ne peuvent pas consulter les attributions, les ensembles d'autorisations, les applications ou les paramètres d'IAM Identity Center. Les principaux auxquels cette politique est attachée ne peuvent effectuer aucune mise à jour dans IAM Identity Center. Par exemple, les principaux disposant de ces autorisations peuvent voir les utilisateurs d'IAM Identity Center, mais ils ne peuvent pas modifier les attributs des utilisateurs ni attribuer de dispositifs MFA.

Pour consulter les autorisations associées à cette politique, reportez-vous AWSSSODirectoryReadOnlyà la section AWS Managed Policy Reference.

AWS politique gérée : AWSIdentitySyncFullAccess

Vous pouvez associer la politique `AWSIdentitySyncFullAccess` à vos identités IAM.

Les principaux auxquels cette politique est attachée disposent d'autorisations d'accès complètes pour créer et supprimer des profils de synchronisation, associer ou mettre à jour un profil de synchronisation à une cible de synchronisation, créer, répertorier et supprimer des filtres de synchronisation, et démarrer ou arrêter la synchronisation.

Détails de l'autorisation

Pour consulter les autorisations associées à cette politique, reportez-vous AWSIdentitySyncFullAccessà la section AWS Managed Policy Reference.

AWS politique gérée : AWSIdentitySyncReadOnlyAccess

Vous pouvez associer la politique `AWSIdentitySyncReadOnlyAccess` à vos identités IAM.

Cette politique accorde des autorisations en lecture seule qui permettent aux utilisateurs de consulter les informations relatives au profil de synchronisation des identités, aux filtres et aux paramètres cibles. Les principaux auxquels cette politique est attachée ne peuvent pas mettre à jour les

paramètres de synchronisation. Par exemple, les principaux disposant de ces autorisations peuvent consulter les paramètres de synchronisation des identités, mais ne peuvent modifier aucune des valeurs de profil ou de filtre.

Pour consulter les autorisations associées à cette politique, reportez-vous AWSIdentitySyncReadOnlyAccessà la section AWS Managed Policy Reference.

AWS politique gérée : AWSSSOServiceRolePolicy

Vous ne pouvez pas associer la `AWSSSOServiceRolePolicy` politique à vos identités IAM.

Cette politique est associée à un rôle lié à un service qui permet à IAM Identity Center de déléguer et d'appliquer les utilisateurs disposant d'un accès par authentification unique à un domaine spécifique. Comptes AWS AWS Organizations Lorsque vous activez IAM, un rôle lié à un service est créé Comptes AWS dans l'ensemble de votre organisation. IAM Identity Center crée également le même rôle lié au service dans chaque compte ajouté ultérieurement à votre organisation. Ce rôle permet à IAM Identity Center d'accéder aux ressources de chaque compte en votre nom. Les rôles liés à un service créés dans chacun d'eux Compte AWS sont nommés. `AWSServiceRoleForSSO` Pour plus d'informations, consultez Utilisation de rôles liés à un service pour IAM Identity Center.

AWS politique gérée : AWSIAMIdentityCenterAllowListForIdentityContext

Lorsque vous assumez un rôle dans le contexte d'identité de l'IAM Identity Center, AWS Security Token Service (AWS STS) attache automatiquement la `AWSIAMIdentityCenterAllowListForIdentityContext` politique au rôle.

Cette politique fournit la liste des actions autorisées lorsque vous utilisez la propagation d'identité sécurisée avec des rôles assumés dans le contexte d'identité IAM Identity Center. Toutes les autres actions appelées dans ce contexte sont bloquées. Le contexte d'identité est transmis en tant que`ProvidedContext`.

Pour consulter les autorisations associées à cette politique, reportez-vous AWSIAMIdentityCenterAllowListForIdentityContextà la section AWS Managed Policy Reference.

Mises à jour des politiques AWS gérées par IAM Identity Center

Le tableau suivant décrit les mises à jour apportées aux politiques AWS gérées pour IAM Identity Center depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page d'historique des documents d'IAM Identity Center.

Modification	Description	Date
AWSIAMIdentityCenterAllowListForIdentityContext	Cette politique inclut désormais les`elasticmapreduce:AddJobFlowSteps` ,, `elasticmapreduce:DescribeCluster` `elasticmapreduce:CancelSteps` `elasticmapreduce:DescribeStep` , et les `elasticmapreduce:ListSteps` actions visant à soutenir la propagation d'identités fiables dans Amazon EMR.	17 mai 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Cette politique inclut désormais les`qapps:CreateQApp` ,,,`qapps:PredictProblemStatementFromConversation` ,,`qapps:PredictQAppFromProblemStatement` ,`qapps:CopyQApp` ,`qapps:GetQApp` ,,`qapps:ListQApps` ,`qapps:UpdateQApp` ,`qapps:DeleteQApp` ,,`qapps:AssociateQAppWithUser` ,`qapps:DisassociateQAppFromUser` ,,`qapps:ImportDocumentToQApp` ,`qapps:Imp`	30 avril 2024

Modification	Description	Date
	`ortDocumentToQAppSession` ,`qapps:CreateLibraryItem` ,, `qapps:GetLibraryItem` `qapps:UpdateLibraryItem` `qapps:CreateLibraryItemReview` `qapps:ListLibraryItems` `qapps:CreateSubscriptionToken` `qapps:StartQAppSession` , et les `qapps:StopQAppSession` actions visant à prendre en charge les sessions de console basées sur l'identité pour les applications AWS gérées qui prennent en charge ces sessions.	
AWSSSOMasterAccountAdministrator	Cette politique inclut désormais les `signin:ListTrustedIdentityPropagationApplicationsForConsole` actions `signin:CreateTrustedIdentityPropagationApplicationForConsole` et destinées à prendre en charge les sessions de console sensibles à l'identité pour les applications AWS gérées qui prennent en charge ces sessions.	26 avril 2024

Modification	Description	Date
AWSSSOMemberAccountAdministrator	Cette politique inclut désormais les `signin:ListTrustedIdentityPropagationApplicationsForConsole` actions `signin:CreateTrustedIdentityPropagationApplicationForConsole` et destinées à prendre en charge les sessions de console sensibles à l'identité pour les applications AWS gérées qui prennent en charge ces sessions.	26 avril 2024
AWSSSOReadOnly	Cette politique inclut désormais l'`signin:ListTrustedIdentityPropagationApplicationsForConsole` action visant à prendre en charge les sessions de console sensibles à l'identité pour les applications AWS gérées qui prennent en charge ces sessions.	26 avril 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Cette politique inclut désormais l'`qbusiness:PutFeedback` action visant à prendre en charge les sessions de console sensibles à l'identité pour les applications AWS gérées qui prennent en charge ces sessions.	26 avril 2024

Modification	Description	Date
AWSIAMIdentityCenterAllowListForIdentityContext	Cette politique inclut désormais les`q:StartConversation` ,,,,`q:SendMessage` , `q:ListConversations` `q:GetConversation` `q:StartTroubleshootingAnalysis` `q:GetTroubleshootingResults` `q:StartTroubleshootingResolutionExplanation` , et les `q:UpdateTroubleshootingCommandResult` actions visant à prendre en charge les sessions de console sensibles à l'identité pour les applications AWS gérées qui prennent en charge ces sessions.	24 avril 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Cette politique inclut désormais l'`sts:SetContext` action visant à prendre en charge les sessions de console sensibles à l'identité pour les applications AWS gérées qui prennent en charge ces sessions.	19 avril 2024

Modification	Description	Date
AWSIAMIdentityCenterAllowListForIdentityContext	Cette politique inclut désormais les `qbusiness:Chat` ,, `qbusiness:ChatSync` `qbusiness:ListConversations` `qbusiness:ListMessages` , et les `qbusiness:DeleteConversation` actions visant à prendre en charge les sessions de console sensibles à l'identité pour les applications AWS gérées qui prennent en charge ces sessions.	11 avril 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Cette politique inclut désormais les `s3:GetDataAccess` actions `s3:GetAccessGrantsInstanceForPrefix` et.	26 novembre 2023
AWSIAMIdentityCenterAllowListForIdentityContext	Cette politique fournit la liste des actions autorisées lorsque vous utilisez la propagation d'identité sécurisée avec des rôles assumés dans le contexte d'identité IAM Identity Center.	15 novembre 2023

Modification	Description	Date
AWSSSODirectoryReadOnly	Cette politique inclut désormais le nouvel espace de noms `identitystore-auth` avec de nouvelles autorisations permettant aux utilisateurs de répertorier et d'obtenir des sessions.	21 février 2023
AWSSSOServiceRolePolicy	Cette politique permet désormais de `UpdateSAMLProvider` prendre des mesures sur le compte de gestion.	20 octobre 2022
AWSSSOMasterAccountAdministrator	Cette politique inclut désormais le nouvel espace de noms `identitystore-auth` avec de nouvelles autorisations permettant à l'administrateur de répertorier et de supprimer les sessions d'un utilisateur.	20 octobre 2022
AWSSSOMemberAccountAdministrator	Cette politique inclut désormais le nouvel espace de noms `identitystore-auth` avec de nouvelles autorisations permettant à l'administrateur de répertorier et de supprimer les sessions d'un utilisateur.	20 octobre 2022

Modification	Description	Date
AWSSSODirectoryAdministrator	Cette politique inclut désormais le nouvel espace de noms `identitystore-auth` avec de nouvelles autorisations permettant à l'administrateur de répertorier et de supprimer les sessions d'un utilisateur.	20 octobre 2022
AWSSSOMasterAccountAdministrator	Cette politique inclut désormais de nouvelles autorisations `ListDelegatedAdministrators` d'appel AWS Organizations. Cette politique inclut également désormais un sous-ensemble d'autorisations `AWSSSOManageDelegatedAdministrator` qui inclut les autorisations d'appeler `RegisterDelegatedAdministrator` et`DeregisterDelegatedAdministrator`.	16 août 2022

Modification	Description	Date
AWSSSOMemberAccountAdministrator	Cette politique inclut désormais de nouvelles autorisations ListDelegatedAdministrators d'appel AWS Organizations. Cette politique inclut également désormais un sous-ensemble d'autorisations AWSSSOManageDelegatedAdministrator qui inclut les autorisations d'appeler RegisterDelegatedAdministrator etDeregisterDelegatedAdministrator .	16 août 2022
AWSSSOReadOnly	Cette politique inclut désormais de nouvelles autorisations ListDelegatedAdministrators d'appel AWS Organizations.	11 août 2022
AWSSSOServiceRolePolicy	Cette politique inclut désormais de nouvelles autorisations pour appeler DeleteRolePermissionsBoundary etPutRolePermisionsBoundary .	14 juillet 2022

Modification	Description	Date
AWSSSOServiceRolePolicy	Cette politique inclut désormais de nouvelles autorisations qui autorisent les appels `ListAWSServiceAccessForOrganization` and `ListDelegatedAdministrators` entrants AWS Organizations.	11 mai 2022
AWSSSOMasterAccountAdministrator AWSSSOMemberAccountAdministrator AWSSSOReadOnly	Ajoutez des autorisations IAM Access Analyzer qui permettent au principal d'utiliser les contrôles de politique à des fins de validation.	28 avril 2022
AWSSSOMasterAccountAdministrator	Cette politique autorise désormais toutes les actions du service IAM Identity Center Identity Store. Pour plus d'informations sur les actions disponibles dans le service IAM Identity Center Identity Store, consultez le document de référence de l'API IAM Identity Center Identity Store.	29 mars 2022
AWSSSOMemberAccountAdministrator	Cette politique autorise désormais toutes les actions du service IAM Identity Center Identity Store.	29 mars 2022

Modification	Description	Date
AWSSSODirectoryAdministrator	Cette politique autorise désormais toutes les actions du service IAM Identity Center Identity Store.	29 mars 2022
AWSSSODirectoryReadOnly	Cette politique donne désormais accès aux actions de lecture du service IAM Identity Center Identity Store. Cet accès est nécessaire pour récupérer les informations relatives aux utilisateurs et aux groupes à partir du service IAM Identity Center Identity Store.	29 mars 2022
AWSIdentitySyncFullAccess	Cette politique permet un accès complet aux autorisations de synchronisation des identités.	3 mars 2022
AWSIdentitySyncReadOnlyAccess	Cette politique accorde des autorisations en lecture seule qui permettent au principal de consulter les paramètres de synchronisation des identités.	3 mars 2022
AWSSSOReadOnly	Cette politique accorde des autorisations en lecture seule qui permettent au principal de consulter les paramètres de configuration d'IAM Identity Center.	4 août 2021

Modification	Description	Date
IAM Identity Center a commencé à suivre les modifications	IAM Identity Center a commencé à suivre les modifications apportées aux politiques AWS gérées.	4 août 2021

Utilisation de rôles liés à un service pour IAM Identity Center

AWS IAM Identity Center utilise des AWS Identity and Access Management rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à IAM Identity Center. Il est prédéfini par IAM Identity Center et inclut toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom. Pour plus d'informations, consultez Rôles liés à un service.

Un rôle lié à un service facilite la configuration d'IAM Identity Center, car il n'est pas nécessaire d'ajouter manuellement les autorisations nécessaires. IAM Identity Center définit les autorisations associées à son rôle lié au service et, sauf indication contraire, seul IAM Identity Center peut assumer ce rôle. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés aux services, consultez Services AWS fonctionnant avec IAM et recherchez les services où Oui figure dans la colonne Rôle lié à un service. Choisissez un Yes (oui) ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations de rôle liées au service pour IAM Identity Center

IAM Identity Center utilise le rôle lié au service nommé AWSServiceRoleForSSOpour accorder à IAM Identity Center les autorisations nécessaires à la gestion des AWS ressources, notamment les rôles IAM, les politiques et l'IdP SAML en votre nom.

Le rôle AWSServiceRoleForSSO lié à un service fait confiance aux services suivants pour assumer le rôle :

- `IAM Identity Center`

La politique d'autorisation des rôles AWSServiceRoleForSSO liés au service permet à IAM Identity Center d'effectuer les tâches suivantes concernant les rôles situés sur le chemin « /aws-reserved/sso.amazonaws.com/ » et avec le préfixe de nom « _ » : AWSReservedSSO

- `iam:AttachRolePolicy`
- `iam:CreateRole`
- `iam:DeleteRole`
- `iam:DeleteRolePermissionsBoundary`
- `iam:DeleteRolePolicy`
- `iam:DetachRolePolicy`
- `iam:GetRole`
- `iam:ListRolePolicies`
- `iam:PutRolePolicy`
- `iam:PutRolePermissionsBoundary`
- `iam:ListAttachedRolePolicies`

La politique d'autorisation des rôles AWSServiceRoleForSSO liés au service permet à IAM Identity Center d'effectuer les opérations suivantes sur les fournisseurs SAML dont le préfixe de nom est « _ » : AWSSSO

- `iam:CreateSAMLProvider`
- `iam:GetSAMLProvider`
- `iam:UpdateSAMLProvider`
- `iam:DeleteSAMLProvider`

La politique d'autorisation des rôles AWSServiceRoleForSSO liés au service permet à IAM Identity Center d'effectuer les tâches suivantes pour toutes les organisations :

- `organizations:DescribeAccount`
- `organizations:DescribeOrganization`
- `organizations:ListAccounts`
- `organizations:ListAWSServiceAccessForOrganization`
- `organizations:ListDelegatedAdministrators`

La politique d'autorisation des rôles AWSServiceRoleForSSO liés au service permet à IAM Identity Center d'effectuer les opérations suivantes pour tous les rôles IAM (*) :

- `iam:listRoles`

La politique d'autorisation des rôles AWSServiceRoleForSSO liés au service permet à IAM Identity Center d'effectuer les opérations suivantes sur « arn:aws:iam : :*:role/ /sso.amazonaws.com/ » : aws-service-role AWSServiceRoleForSSO

- `iam:GetServiceLinkedRoleDeletionStatus`
- `iam:DeleteServiceLinkedRole`

La politique d'autorisation des rôles permet à IAM Identity Center d'effectuer les actions suivantes sur les ressources.

```
{
   "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":[
               "*"
            ]
         }
      ]
}
```

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour IAM Identity Center

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Une fois activé, IAM Identity Center crée un rôle lié à un service dans tous les comptes de l'organisation dans Organizations. AWS IAM Identity Center crée également le même rôle lié au service dans chaque compte ajouté ultérieurement à votre organisation. Ce rôle permet à IAM Identity Center d'accéder aux ressources de chaque compte en votre nom.

Remarques

- Si vous êtes connecté au compte de AWS Organizations gestion, celui-ci utilise votre rôle actuellement connecté et non le rôle lié au service. Cela empêche l'escalade des privilèges.
- Lorsque IAM Identity Center effectue des opérations IAM dans le compte de AWS Organizations gestion, toutes les opérations sont effectuées à l'aide des informations d'identification du principal IAM. Cela permet aux connexions de CloudTrail savoir qui a effectué tous les changements de privilèges dans le compte de gestion.

Important

Si vous utilisiez le service IAM Identity Center avant le 7 décembre 2017, date à laquelle il a commencé à prendre en charge les rôles liés au service, IAM Identity Center a créé le AWSServiceRoleForSSO rôle dans votre compte. Pour plus d'informations, consultez A New Role Appeared in My IAM Account (Un nouveau rôle est apparu dans mon compte IAM).

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour le recréer dans votre compte.

Modification d'un rôle lié à un service pour IAM Identity Center

IAM Identity Center ne vous permet pas de modifier le rôle lié au AWSServiceRoleForSSO service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour IAM Identity Center

Il n'est pas nécessaire de supprimer le AWSServiceRoleForSSO rôle manuellement. Lorsqu'un Compte AWS est supprimé d'une AWS organisation, IAM Identity Center nettoie automatiquement les ressources et en supprime le rôle lié au service. Compte AWS

Vous pouvez également utiliser la console IAM, la CLI IAM ou l'API IAM pour supprimer manuellement le rôle lié à un service. Pour cela, vous devez commencer par nettoyer les ressources de votre rôle lié à un service. Vous pouvez ensuite supprimer ce rôle manuellement.

> **Note**
>
> Si le service IAM Identity Center utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer les ressources IAM Identity Center utilisées par le AWSServiceRoleForSSO

1. Supprimer l'accès des utilisateurs et des groupespour tous les utilisateurs et groupes ayant accès au Compte AWS.
2. Supprimer des ensembles d'autorisationsque vous avez associé au Compte AWS.

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, la CLI IAM ou l'API IAM pour supprimer le rôle lié au AWSServiceRoleForSSO service. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Autorisation de la console et de l'API IAM Identity Center

Les API de console IAM Identity Center existantes prennent en charge la double autorisation, ce qui vous permet de continuer à utiliser les opérations d'API existantes lorsque de nouvelles API sont disponibles. Si vous possédez des instances d'IAM Identity Center créées avant le 15 novembre 2023 et le 15 octobre 2020, vous pouvez utiliser les tableaux suivants pour déterminer quelles opérations d'API correspondent désormais aux opérations d'API plus récentes publiées après ces dates.

Rubriques

- Actions relatives à l'API après novembre 2023
- Actions de l'API après octobre 2020

Actions relatives à l'API après novembre 2023

Les instances d'IAM Identity Center créées avant le 15 novembre 2023 honorent à la fois les anciennes et les nouvelles actions d'API, à condition qu'aucune de ces actions ne soit explicitement refusée. Les instances créées après le 15 novembre 2023 utilisent des actions d'API plus récentes pour l'autorisation dans la console IAM Identity Center.

Nom du fonctionnement de la console utilisé avant le 15 novembre 2023	Action API utilisée après le 15 novembre 2023
AssociateProfile	CreateApplicationAssignment
CreateManagedApplicationInstance | CreateApplicationInstance	CreateApplication
CreateManagedApplicationInstance	PutApplicationAuthenticationMethod
DeleteApplicationInstance | DeleteManagedApplicationInstance	DeleteApplication
DeleteSSO	DeleteInstance
DisassociateProfile	DeleteApplicationAssignment
GetApplicationTemplate	DescribeApplicationProvider
GetManagedApplicationInstance	DescribeApplication
GetSharedSsoConfiguration	DescribeInstance
ListApplicationInstances	ListApplications
ListApplicationTemplates	ListApplicationProviders
ListDirectoryAssociations	DescribeInstance
ListProfileAssociations	ListApplicationAssignments

Nom du fonctionnement de la console utilisé avant le 15 novembre 2023	Action API utilisée après le 15 novembre 2023
UpdateApplicationInstanceDisplayData | UpdateApplicationInstanceStatus | UpdateManagedApplicationInstanceStatus	UpdateApplication

Actions de l'API après octobre 2020

Les instances d'IAM Identity Center créées avant le 15 octobre 2020 honorent les anciennes et les nouvelles actions d'API, à condition qu'aucune de ces actions ne soit explicitement refusée. Les instances créées après le 15 octobre 2020 utilisent des actions d'API plus récentes pour l'autorisation dans la console IAM Identity Center.

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
AssociateProfile	AssociateProfile	CreateAccountAssignment
AttachManagedPolicy	PutPermissionsPolicy	AttachManagedPolicyToPermissionSet
CreatePermissionSet	CreatePermissionSet	CreatePermissionSet
DeleteApplicationInstanceForAWsAccount	DeleteApplicationInstance | DeleteTrust	DeleteAccountAssignment
DeleteApplicationProfileForAwsAccount	DeleteProfile	DeleteAccountAssignment
DeletePermissionsPolicy	DeletePermissionsPolicy	DeleteInlinePolicyFromPermissionSet
DeletePermissionSet	DeletePermissionSet	DeletePermissionSet
DescribePermissionsPolicies	DescribePermissionsPolicies	ListManagedPoliciesInPermissionSet

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
DetachManagedPolicy	DeletePermissionsPolicy	DetachManagedPolicyFromPermissionSet
DisassociateProfile	DisassociateProfile	DeleteAccountAssignment
GetApplicationInstanceForAWSAccount	GetApplicationInstance	ListAccountAssignments
GetAWSAccountProfileStatus	GetProfile	ListPermissionSetsProvisionedToAccount
GetPermissionSet	GetPermissionSet	DescribePermissionSet
GetPermissionsPolicy	GetPermissionsPolicy	GetInlinePolicyForPermissionSet
ListAccountsWithProvisionedPermissionSet	ListApplicationInstances | GetApplicationInstance	ListAccountsForProvisionedPermissionSet
ListAWSAccountProfiles	ListProfiles | GetProfile	ListPermissionSetsProvisionedToAccount
ListPermissionSets	ListPermissionSets	ListPermissionSets
ListProfileAssociations	ListProfileAssociations	ListAccountAssignments
ProvisionApplicationInstanceForAWSAccount	GetApplicationInstance | CreateApplicationInstance	CreateAccountAssignment
ProvisionApplicationProfileForAWSAccountInstance	GetProfile | CreateProfile | UpdateProfile	CreateAccountAssignment
ProvisionSAMLProvider	GetTrust | CreateTrust | UpdateTrust	CreateAccountAssignment
PutPermissionsPolicy	PutPermissionsPolicy	PutInlinePolicyToPermissionSet

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
UpdatePermissionSet	UpdatePermissionSet	UpdatePermissionSet

AWS STS clés contextuelles de condition pour IAM Identity Center

Lorsqu'un principal fait une demande à AWS, AWS rassemble les informations de la demande dans un contexte de demande, qui est utilisé pour évaluer et autoriser la demande. Vous pouvez utiliser l'élément `Condition` d'une politique JSON pour comparer des clés dans le contexte de demande avec les valeurs de clé spécifiées dans votre politique. Les informations relatives à la demande sont fournies par différentes sources, notamment le principal auteur de la demande, la ressource, la demande pour laquelle elle est faite et les métadonnées relatives à la demande elle-même. Les clés de condition spécifiques au service sont définies pour être utilisées avec un service individuel AWS .

IAM Identity Center inclut un fournisseur de AWS STS contexte qui permet aux applications AWS gérées et aux applications tierces d'ajouter des valeurs aux clés de condition définies par IAM Identity Center. Ces clés sont incluses dans les rôles IAM. Les valeurs clés sont définies lorsqu'une application transmet un jeton à AWS STS. L'application obtient le jeton auquel elle passe de AWS STS l'une des manières suivantes :

- Lors de l'authentification auprès d'IAM Identity Center.
- Après échange de jetons avec un émetteur de jetons de confiance pour une propagation d'identité fiable. Dans ce cas, l'application obtient un jeton auprès d'un émetteur de jetons fiable et échange ce jeton contre un jeton auprès d'IAM Identity Center.

Ces clés sont généralement utilisées par les applications qui s'intègrent à la propagation d'identité sécurisée. Dans certains cas, lorsque des valeurs clés sont présentes, vous pouvez utiliser ces clés dans les politiques IAM que vous créez pour autoriser ou refuser des autorisations.

Par exemple, vous souhaiterez peut-être fournir un accès conditionnel à une ressource en fonction de la valeur de`UserId`. Cette valeur indique quel utilisateur IAM Identity Center utilise le rôle. L'exemple est similaire à l'utilisation de`SourceId`. Contrairement à `SourceId` ce qui se passe, la valeur pour `UserId` représente un utilisateur spécifique vérifié dans le magasin d'identités. Cette valeur est présente dans le jeton que l'application obtient puis transmet. AWS STS Il ne s'agit pas d'une chaîne à usage général qui peut contenir des valeurs arbitraires.

Rubriques

boutique d'identité : UserId

Cette clé de contexte est celle `UserId` de l'utilisateur IAM Identity Center qui fait l'objet de l'assertion de contexte émise par IAM Identity Center. L'assertion de contexte est transmise à AWS STS. Vous pouvez utiliser cette clé pour comparer l'identifiant `UserId` de l'utilisateur IAM Identity Center au nom duquel la demande est faite avec l'identifiant de l'utilisateur que vous spécifiez dans la politique.

- Disponibilité : cette clé est incluse dans le contexte de la demande après la définition d'une assertion de contexte émise par IAM Identity Center, lorsqu'un rôle est assumé à l'aide d'une AWS STS `assume-role` commande quelconque dans le cadre de l'opération AWS CLI ou de l' AWS STS `AssumeRole`API.
- Type de données : chaîne
- Type de valeur – À valeur unique

boutique d'identité : IdentityStoreArn

Cette clé de contexte est l'ARN de la banque d'identités attachée à l'instance d'IAM Identity Center qui a émis l'assertion de contexte. C'est également le magasin d'identité dans lequel vous pouvez rechercher des attributs`identitystore:UserID`. Vous pouvez utiliser cette clé dans les politiques pour déterminer si elle `identitystore:UserID` provient d'un ARN de magasin d'identités attendu.

- Disponibilité : cette clé est incluse dans le contexte de la demande après la définition d'une assertion de contexte émise par IAM Identity Center, lorsqu'un rôle est assumé à l'aide d'une AWS STS `assume-role` commande quelconque dans le cadre de l'opération AWS CLI ou de l' AWS STS `AssumeRole`API.
- Type de données : Arn, String
- Type de valeur – À valeur unique

centre d'identité : ApplicationArn

Cette clé de contexte est l'ARN de l'application à laquelle IAM Identity Center a émis une assertion de contexte. Vous pouvez utiliser cette clé dans les politiques pour déterminer si elle `identitycenter:ApplicationArn` provient d'une application attendue. L'utilisation de cette clé peut aider à empêcher une application inattendue d'accéder à un rôle IAM.

- Disponibilité — Cette clé est incluse dans le contexte de demande d'une opération d' AWS STS `AssumeRole`API. Le contexte de demande inclut une assertion de contexte émise par IAM Identity Center.
- Type de données : Arn, String
- Type de valeur – À valeur unique

centre d'identité : CredentialId

Cette clé de contexte est un identifiant aléatoire pour les informations d'identification du rôle à identité améliorée et est utilisée uniquement pour la journalisation. Cette valeur clé étant imprévisible, nous vous recommandons de ne pas l'utiliser pour les assertions contextuelles dans les politiques.

- Disponibilité — Cette clé est incluse dans le contexte de demande d'une opération d' AWS STS `AssumeRole`API. Le contexte de demande inclut une assertion de contexte émise par IAM Identity Center.
- Type de données : chaîne
- Type de valeur – À valeur unique

centre d'identité : InstanceArn

Cette clé de contexte est l'ARN de l'instance d'IAM Identity Center qui a émis l'assertion de contexte pour. `identitystore:UserID` Vous pouvez utiliser cette clé pour déterminer si l'assertion de contexte `identitystore:UserID` et provient d'un ARN d'instance IAM Identity Center attendu.

- Disponibilité — Cette clé est incluse dans le contexte de demande d'une opération d' AWS STS `AssumeRole`API. Le contexte de demande inclut une assertion de contexte émise par IAM Identity Center.
- Type de données : Arn, String
- Type de valeur – À valeur unique

Journalisation et surveillance dans IAM Identity Center

La bonne pratique consiste à surveiller votre organisation pour vous assurer que les modifications sont journalisées. Cela vous permet de vous assurer que tout changement inattendu peut être étudié et que les modifications indésirables peuvent être annulées. AWS IAM Identity Center prend actuellement en charge deux AWS services qui vous aident à surveiller votre organisation et les activités qui s'y déroulent.

Rubriques

Journalisation des appels d'API IAM Identity Center avec AWS CloudTrail

AWS IAM Identity Center est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans IAM Identity Center. CloudTrail capture les appels d'API pour IAM Identity Center sous forme d'événements. Les appels capturés incluent des appels provenant de la console IAM Identity Center et des appels de code vers les opérations de l'API IAM Identity Center. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour IAM Identity Center. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à IAM Identity Center, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des informations supplémentaires.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Rubriques

Informations sur le centre d'identité IAM dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans IAM Identity Center, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements survenus dans votre entreprise Compte AWS, y compris ceux relatifs à IAM Identity Center, créez un historique. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal de suivi dans la console, il s'applique à toutes les régions AWS . Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Présentation de la création d'un journal de suivi
- CloudTrail services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Lorsque la CloudTrail journalisation est activée dans vos actions Compte AWS, les appels d'API effectués aux actions d'IAM Identity Center sont suivis dans des fichiers journaux. Les enregistrements IAM Identity Center sont écrits avec les autres enregistrements AWS de service dans un fichier journal. CloudTrail détermine à quel moment créer et écrire dans un nouveau fichier en fonction d'une période et de la taille du fichier.

Les CloudTrail opérations IAM Identity Center suivantes sont prises en charge :

Opérations de l'API de console	Opérations d'API publiques
`AssociateDirectory`	`AttachManagedPolicyToPermissionSet`

Opérations de l'API de console	Opérations d'API publiques
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
DisassociateProfile	ListAccountAssignmentCreationStatus

Opérations de l'API de console	Opérations d'API publiques
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
PutMfaDeviceManagementForDirectory	UpdatePermissionSet
PutPermissionsPolicy	

Opérations de l'API de console	Opérations d'API publiques
StartSSO	
UpdateApplicationInstanceActiveCertificate	
UpdateApplicationInstanceDisplayData	
UpdateApplicationInstanceServiceProviderConfiguration	
UpdateApplicationInstanceStatus	
UpdateApplicationInstanceResponseConfiguration	
UpdateApplicationInstanceResponseSchemaConfiguration	
UpdateApplicationInstanceSecurityConfiguration	
UpdateDirectoryAssociation	
UpdateProfile	

Pour plus d'informations sur les opérations d'API publiques d'IAM Identity Center, consultez le Guide de référence des API IAM Identity Center.

Les CloudTrail opérations IAM Identity Center Identity Store suivantes sont prises en charge :

- 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

Les actions IAM Identity Center OIDC suivantes sont CloudTrail prises en charge :

- `CreateToken`
- `RegisterClient`
- `StartDeviceAuthorization`

Les actions suivantes du portail IAM Identity Center sont CloudTrail prises en charge :

- `Authenticate`
- `Federate`
- `ListApplications`
- `ListProfilesForApplication`
- `ListAccounts`
- `ListAccountRoles`
- `GetRoleCredentials`
- `Logout`

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été faite avec les informations d'identification de l'utilisateur root ou de l'utilisateur AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour plus d'informations, consultez l'élément CloudTrail UserIdentity.

Comprendre les entrées du fichier journal d'IAM Identity Center

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent

pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal pour un administrateur (samadams@example.com) qui a eu lieu dans la console IAM Identity Center :


```
{
   "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"
      }
   ]
}
```


L'exemple suivant montre une entrée de CloudTrail journal pour une action de l'utilisateur final (bobsmith@example.com) qui a eu lieu sur le portail AWS d'accès :

```
{
   "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"
      }
   ]
}
```

L'exemple suivant montre une entrée de CloudTrail journal pour une action de l'utilisateur final (bobsmith@example.com) qui a eu lieu dans IAM Identity Center OIDC :

```
{
      "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"
}
```


Comprendre les événements de connexion à IAM Identity Center

AWS CloudTrail enregistre les événements de connexion réussis et infructueux pour toutes les sources AWS IAM Identity Center d'identité. Les identités issues du SSO natif et d'Active Directory (AD Connector et AWS Managed Microsoft AD) incluront des événements de connexion supplémentaires qui sont capturés chaque fois qu'un utilisateur est invité à résoudre un défi ou un facteur d'identification spécifique, ainsi que le statut de cette demande de vérification d'identification en particulier. Ce n'est qu'une fois qu'un utilisateur a terminé tous les tests d'identification requis qu'il sera connecté, ce qui entraînera l'enregistrement d'un `UserAuthentication` événement.

Le tableau suivant présente les noms de chacun des CloudTrail événements de connexion à IAM Identity Center, leur objectif et leur applicabilité aux différentes sources d'identité.

Nom de l'événement	But de l'événement	Applicabilité de la source d'identité
`CredentialChallenge`	Utilisé pour indiquer qu'IAM Identity Center a demandé à l'utilisateur de résoudre un problème d'identif ication spécifique et indique `CredentialType` ce qui était requis (par exemple, PASSWORD ou TOTP).	Utilisateurs natifs d'IAM Identity Center, AD Connector et AWS Managed Microsoft AD
`CredentialVerifica tion`	Utilisé pour indiquer que l'utilisateur a tenté de résoudre une `CredentialChalleng e` demande spécifique et indique si cet identifiant a réussi ou échoué.	Utilisateurs natifs d'IAM Identity Center, AD Connector et AWS Managed Microsoft AD
`UserAuthentication`	Utilisé pour indiquer que toutes les exigences d'authent ification auxquelles l'utilisa teur a été confronté ont été satisfaites avec succès et que l'utilisateur s'est connecté avec succès. Si les utilisate urs ne parviennent pas à relever les défis d'identification requis, aucun *`UserAuthe ntication`* événement ne sera enregistré.	Toutes les sources d'identité

Le tableau suivant présente d'autres champs de données d'événements utiles contenus dans des CloudTrail événements de connexion spécifiques.

Nom de l'événement	But de l'événement	Applicabilité dans un événement de connexion	Exemples de valeur
`AuthWorkflowID`	Utilisé pour corréler tous les événements émis sur l'ensemble d'une séquence de connexion. Pour chaque connexion utilisateur, plusieurs événements peuvent être émis par IAM Identity Center.	`CredentialChallenge` , `CredentialVerification` , `UserAuthentication`	« AuthWorkflow Identifiant » : « 9de74b32-8362-4a01-a524-de21df59fd83 »
`CredentialType`	Utilisé pour spécifier l'identifiant ou le facteur contesté. `UserAuthentication` les événements incluront toutes les `CredentialType` valeurs qui ont été vérifiées avec succès tout au long de la séquence de connexion de l'utilisateur.	`CredentialChallenge` , `CredentialVerification` , `UserAuthentication`	CredentialType« : « PASSWORD » ou "CredentialType« : « PASSWORD, TOTP » (les valeurs possibles incluent : PASSWORD, TOTP, WEBAUTHN, EXTERNAL_IDP, RESYNC_TOTP)
`DeviceEnrollmentRequired`	Utilisé pour spécifier que l'utilisateur devait enregistrer un dispositif MFA lors de la connexion et qu'il a correctement répondu à cette demande.	`UserAuthentication`	DeviceEnrollmentRequired« : « vrai »

Nom de l'événement	But de l'événement	Applicabilité dans un événement de connexion	Exemples de valeur
`LoginTo`	Utilisé pour spécifier l'emplacement de la redirection après une séquence de connexion réussie.	`UserAuthentication`	« LoginTo « : https://mydirectory.awsapps.com/start/... »

Exemples d'événements pour les scénarios de connexion à IAM Identity Center

Les exemples suivants montrent la séquence d' CloudTrail événements attendue pour différents scénarios de connexion.

Rubriques

- Connexion réussie lors de l'authentification uniquement avec un mot de passe
- Connexion réussie lors de l'authentification auprès d'un fournisseur d'identité externe
- Connexion réussie lors de l'authentification à l'aide d'un mot de passe et d'une application d'authentification TOTP
- Une connexion réussie est requise lorsque vous vous authentifiez avec un mot de passe et que l'enregistrement MFA est obligatoire
- Échec de connexion lors de l'authentification avec un seul mot de passe

Connexion réussie lors de l'authentification uniquement avec un mot de passe

La séquence d'événements suivante présente un exemple de connexion réussie uniquement par mot de passe.

CredentialChallenge (Mot de passe)


```
{
   "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"
   }
}
```


Succès CredentialVerification (mot de passe)


```
{
   "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"
   }
}
```


UserAuthentication Réussite (mot de passe uniquement)


```
{
   "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"
   }
}
```


Connexion réussie lors de l'authentification auprès d'un fournisseur d'identité externe

La séquence d'événements suivante présente un exemple de connexion réussie lors d'une authentification via le protocole SAML à l'aide d'un fournisseur d'identité externe.

UserAuthentication Succès (fournisseur d'identité externe)


```
{
   "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"
   }
}
```


Connexion réussie lors de l'authentification à l'aide d'un mot de passe et d'une application d'authentification TOTP

La séquence d'événements suivante illustre un exemple où une authentification multifactorielle était requise lors de la connexion et où l'utilisateur s'est connecté avec succès à l'aide d'un mot de passe et d'une application d'authentification TOTP.

CredentialChallenge (Mot de passe)


```
{
   "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"
   }
}
```

Succès CredentialVerification (mot de passe)

```
{
   "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"
   }
}
```

Succès 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"
   }
}
```

UserAuthentication Réussi (mot de passe + 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"
   }
}
```

Une connexion réussie est requise lorsque vous vous authentifiez avec un mot de passe et que l'enregistrement MFA est obligatoire

La séquence d'événements suivante montre un exemple de connexion par mot de passe réussie, mais l'utilisateur a été obligé et a réussi à enregistrer un dispositif MFA avant de terminer sa connexion.

CredentialChallenge (Mot de passe)

```
{
   "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"
   }
}
```

Succès CredentialVerification (mot de passe)

```
{
   "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"
   }
}
```

UserAuthentication Réussite (mot de passe et enregistrement MFA requis)

```
{
   "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"
   }
}
```

Échec de connexion lors de l'authentification avec un seul mot de passe

La séquence d'événements suivante présente un exemple d'échec de connexion par mot de passe uniquement.

CredentialChallenge (Mot de passe)

```
{
   "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"
   }
}
```


Echec CredentialVerification (mot de passe)


```
{
   "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 peut travailler avec Amazon EventBridge pour déclencher des événements lorsque des actions spécifiées par l'administrateur se produisent dans une organisation. Par exemple, en raison de la sensibilité de ces actions, la plupart des administrateurs souhaitent être avertis chaque fois que quelqu'un crée un nouveau compte dans l'organisation ou quand un administrateur d'un compte membre tente de quitter l'organisation. Vous pouvez configurer EventBridge des règles qui recherchent ces actions, puis envoient les événements générés à des cibles définies par l'administrateur. Une cible peut être une rubrique Amazon SNS qui envoie des e-mails ou des SMS à ses abonnés. Vous pouvez également créer une AWS Lambda fonction qui enregistre les détails de l'action pour un examen ultérieur.

Pour en savoir plus EventBridge, notamment comment le configurer et l'activer, consultez le guide de EventBridge l'utilisateur Amazon.

Enregistrement des erreurs de synchronisation AD et de synchronisation AD configurables

Vous pouvez activer la connexion sur votre synchronisation Active Directory (AD) et configurer des configurations de synchronisation AD configurables pour recevoir des journaux contenant des informations sur les erreurs susceptibles de se produire pendant le processus de synchronisation. Grâce à ces journaux, vous pouvez vérifier s'il existe un problème avec votre synchronisation AD et la synchronisation AD configurable et prendre des mesures le cas échéant. Vous pouvez envoyer vos journaux vers un groupe de CloudWatch journaux Amazon Logs, un bucket Amazon Simple Storage Service (Amazon S3) ou un Amazon Data Firehose dont la livraison entre comptes est prise en charge pour les buckets Amazon S3 et Firehose.

Pour plus d'informations sur les limitations, les autorisations et les journaux vendus, consultez la section Activation de la journalisation à partir de Services AWS.

> **Note**
>
> La connexion vous est facturée. Pour plus d'informations, consultez Vended Logs sur la page de CloudWatch tarification d'Amazon.

Pour activer la synchronisation AD et les journaux d'erreurs configurables

1. Connectez-vous à la console IAM Identity Center.

2. Sélectionnez Settings (Paramètres).
3. Sur la page Paramètres, choisissez l'onglet Source d'identité, sélectionnez Actions, puis sélectionnez Gérer les journaux.
4. Choisissez Ajouter la livraison du journal et l'un des types de destination suivants.
    a. Choisissez To Amazon CloudWatch Logs. Choisissez ou entrez ensuite le groupe de journaux de destination.
    b. Choisissez To Amazon S3. Choisissez ou entrez ensuite le compartiment de destination.
    c. Choisissez To Firehose. Choisissez ou entrez ensuite le flux de diffusion de destination.
5. Sélectionnez Envoyer.

Pour désactiver la synchronisation AD et les journaux d'erreurs configurables

1. Connectez-vous à la console IAM Identity Center.
2. Sélectionnez Settings (Paramètres).
3. Sur la page Paramètres, choisissez l'onglet Source d'identité, sélectionnez Actions, puis sélectionnez Gérer les journaux.
4. Choisissez Supprimer pour la destination que vous souhaitez supprimer.
5. Sélectionnez Envoyer.

Champs du journal des erreurs de synchronisation AD et de synchronisation AD configurables

Consultez la liste suivante pour connaître les éventuels champs du journal des erreurs.

`sync_profile_name`

Nom du profil de synchronisation.

`error_code`

Le code d'erreur qui représente le type d'erreur qui s'est produit.

`error_message`

Message contenant des informations détaillées sur l'erreur survenue.

`sync_source`

La source de synchronisation est l'endroit à partir duquel les entités sont synchronisées. Pour IAM Identity Center, il s'agit d'un Active Directory (AD) géré par AWS Directory Service. La source de synchronisation contient le domaine et l'ARN du répertoire concerné.

`sync_target`

La cible de synchronisation est la destination où les entités sont enregistrées. Pour IAM Identity Center, il s'agit d'un magasin d'identités. La cible de synchronisation contient l'ARN du magasin d'identités concerné.

`source_entity_id`

Identifiant unique de l'entité à l'origine de l'erreur. Pour IAM Identity Center, il s'agit du SID de l'entité.

`source_entity_type`

Type d'entité à l'origine de l'erreur. La valeur peut être `USER` ou `GROUP`.

`eventTimestamp`

Horodatage auquel l'erreur s'est produite.

Exemples de journaux d'erreurs de synchronisation AD et de synchronisation AD configurable

Exemple 1 : journal des erreurs pour un mot de passe expiré pour un annuaire AD

```
{
    "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"
```

```
}
```

Exemple 2 : journal des erreurs pour un utilisateur dont le nom d'utilisateur n'est pas unique

```
{
    "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"
}
```

Validation de conformité pour IAM Identity Center

Services AWS Des auditeurs tiers évaluent leur sécurité et leur conformité dans AWS IAM Identity Center le cadre de multiples programmes de AWS conformité.

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et fournissent des étapes pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

> **Note**
>
> Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Normes de conformité prises en charge

IAM Identity Center a fait l'objet d'un audit selon les normes suivantes et peut être utilisé dans le cadre de solutions pour lesquelles vous devez obtenir une certification de conformité.

AWS a étendu son programme de conformité à la loi HIPAA (Health Insurance Portability and Accountability Act) pour inclure IAM Identity Center en tant que service éligible à la loi HIPAA.

AWS propose un livre blanc axé sur la loi HIPAA aux clients qui souhaitent en savoir plus sur la manière dont ils peuvent traiter et stocker les informations Services AWS de santé. Pour de plus amples informations, veuillez consulter HIPAA compliance (français non garanti).

Le programme d'évaluateurs enregistrés en matière de sécurité de l'information (IRAP) permet aux clients du gouvernement australien de s'assurer que des contrôles de conformité appropriés sont en place et de détermine r le modèle de responsabilité approprié pour répondre aux exigences du manuel de sécurité des informations (ISM) du gouvernement australien produit par le Centre australien de cybersécurité (ACSC). Pour plus d'informa tions, consultez les ressources de l'IRAP.

IAM Identity Center dispose d'une attestation de conformit é à la norme de sécurité des données (DSS) de l'industrie des cartes de paiement (PCI) version 3.2 au niveau 1 des fournisseurs de services.

Les clients qui utilisent AWS des produits et services pour stocker, traiter ou transmettre les données des titulaires de cartes peuvent utiliser les sources d'identité suivantes dans IAM Identity Center pour gérer leur propre certifica tion de conformité à la norme PCI DSS :

- Active Directory

	• Fournisseur d'identité externe La source d'identité IAM Identity Center n'est actuellement pas conforme à la norme PCI DSS. Pour plus d'informations sur la norme PCI DSS, notamment sur la manière de demander une copie du Package de AWS conformité PCI, consultez la section PCI DSS niveau 1.
	Les rapports de contrôle du système et de l'organisation (SOC) sont des rapports d'examen indépendants réalisés par des tiers qui montrent comment IAM Identity Center atteint les principaux contrôles et objectifs de conformit é. Ces rapports vous aident, ainsi que vos auditeurs, à comprendre comment les contrôles soutiennent les opérations et la conformité. Il existe trois types de rapports SOC : • AWS Rapport SOC 1 - Télécharger avec AWS Artifact • AWS SOC 2 : Rapport sur la sécurité, la disponibilité et la confidentialité - Télécharger avec AWS Artifact • AWS SOC 3 : Rapport sur la sécurité, la disponibilité et la confidentialité IAM Identity Center est concerné par les rapports AWS SOC 1, SOC 2 et SOC 3. Pour plus d'informations, consultez Conformité SOC.

Résilience dans IAM Identity Center

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. AWS Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone de disponibilité à l'autre sans interruption. Les zones

de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section Infrastructure AWS globale.

Pour en savoir plus sur AWS IAM Identity Center la résilience, voirConception de la résilience et comportement régional.

Sécurité de l'infrastructure dans IAM Identity Center

En tant que service géré, AWS IAM Identity Center il est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder à IAM Identity Center via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Balisage de ressources AWS IAM Identity Center

Une balise est une étiquette d'attribut personnalisée que vous ajoutez à une ressource AWS pour faciliter l'identification, l'organisation et la recherche de ressources. Chaque balise se compose de deux parties :

- Une clé de balise (par exemple, `CostCenter`, `Environment` ou `Project`). Une clé de balise est sensible à la casse et peut contenir 128 caractères au plus.
- Une valeur de balise (par exemple, `111122223333` ou `Production`). Les valeurs de balise peuvent comporter jusqu'à 256 caractères et, comme les clés de balise, sont sensibles à la casse. Vous pouvez définir la valeur d'une balise sur une chaîne vide, mais vous ne pouvez pas définir la valeur d'une balise sur null. Si la valeur de balise est omise, cela équivaut à utiliser une chaîne vide.

Les balises vous aident à identifier et organiser vos ressources AWS. De nombreux services AWS prennent en charge le balisage. Vous pouvez donc attribuer la même balise à des ressources à partir de différents services pour indiquer que les ressources sont liées. Par exemple, vous pouvez attribuer la même balise à un ensemble d'autorisations spécifique dans votre instance d'IAM Identity Center. Pour plus d'informations sur les stratégies de balisage, consultez les AWSressources de balisage du Références générales AWSguide et les meilleures pratiques en matière de balisage.

Outre l'identification, l'organisation et le suivi de vos AWS ressources à l'aide de balises, vous pouvez utiliser des balises dans les politiques IAM pour contrôler qui peut consulter vos ressources et interagir avec elles. Pour en savoir plus sur l'utilisation de balises pour contrôler l'accès, consultez la section Contrôle de l'accès aux AWS ressources à l'aide de balises dans le guide de l'utilisateur IAM. Par exemple, vous pouvez autoriser un utilisateur à mettre à jour un ensemble d'autorisations IAM Identity Center, mais uniquement si le jeu d'autorisations IAM Identity Center comporte une `owner` balise dont la valeur correspond au nom de cet utilisateur.

À l'heure actuelle, vous ne pouvez appliquer des balises qu'aux ensembles d'autorisations. Vous ne pouvez pas appliquer de balises aux rôles correspondants créés par IAM Identity Center. Comptes AWS Vous pouvez utiliser la console IAM Identity Center AWS CLI ou les API IAM Identity Center pour ajouter, modifier ou supprimer des balises pour un ensemble d'autorisations.

Les sections suivantes fournissent des informations supplémentaires sur les balises pour IAM Identity Center.

Restrictions liées aux étiquettes

Les restrictions de base suivantes s'appliquent aux balises figurant sur les ressources de l'IAM Identity Center :

- Le nombre maximum de balises que vous pouvez attribuer à une ressource est de 50.
- La longueur de clé maximale est de 128 caractères Unicode.
- La longueur de valeur maximale est de 256 caractères Unicode.
- Les caractères valides pour une clé et une valeur de balise sont les suivants :

  a-z, A-Z, 0-9, espace et les caractères suivants : _. :/= + - et @
- Les clés et les valeurs sont sensibles à la casse.
- N'utilisez pas `aws:` comme préfixe pour les clés ; seul AWS peut utiliser cette valeur.

Gérez les balises à l'aide de la console IAM Identity Center

Vous pouvez utiliser la console IAM Identity Center pour ajouter, modifier et supprimer des balises associées à votre instance ou à vos ensembles d'autorisations.

Pour gérer les ensembles d'autorisations, les balises d'une console IAM Identity Center

1. Ouvrez la console IAM Identity Center.
2. Choisissez Ensembles d'autorisations.
3. Choisissez le nom de l'ensemble d'autorisations contenant les balises que vous souhaitez gérer.
4. Dans l'onglet Autorisations, sous Balises, effectuez l'une des opérations suivantes, puis passez à l'étape suivante :

   a. Si des balises sont déjà attribuées à cet ensemble d'autorisations, choisissez Modifier les balises.

   b. Si aucun tag n'est attribué à cet ensemble d'autorisations, choisissez Ajouter des tags.
5. Pour chaque nouvelle balise, saisissez les valeurs dans les colonnes Clé et Valeur (facultatif). Lorsque vous avez terminé, choisissez Save changes (Enregistrer les modifications).

Pour supprimer une étiquette, choisissez le X dans la colonne Supprimer à côté de la balise que vous souhaitez supprimer.

Pour gérer les balises d'une instance d'IAM Identity Center

1. Ouvrez la console IAM Identity Center.
2. Sélectionnez Settings (Paramètres).
3. Sélectionnez l'onglet Tags (Identifications).
4. Pour chaque balise, saisissez les valeurs dans les champs Clé et Valeur (facultatif). Lorsque vous avez terminé, cliquez sur le bouton Ajouter un nouveau tag.

Pour supprimer une étiquette, cliquez sur le bouton Supprimer à côté de la balise que vous souhaitez supprimer.

Exemples AWS CLI

AWS CLIfournit des commandes que vous pouvez utiliser pour gérer les balises que vous attribuez à votre ensemble d'autorisations.

Affectation de balises

Utilisez les commandes suivantes pour attribuer des balises à votre ensemble d'autorisations.

Example **`tag-resource`**Commande pour un ensemble d'autorisations

Attribuez des balises à un ensemble d'autorisations en utilisant `tag-resource`dans le `sso` jeu de commandes :

```
$ aws sso-admin tag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tags Stage=Test
```

Cette commande comprend les paramètres suivants :

- `instance-arn`— Le nom de ressource Amazon (ARN) de l'instance IAM Identity Center sous laquelle l'opération sera exécutée.
- `resource-arn`— L'ARN de la ressource contenant les balises à répertorier.
- `tags` – Paires clé-valeur des étiquettes.

Pour affecter plusieurs balises à la fois, spécifiez-les dans une liste séparée par des virgules :

```
$ aws sso-admin tag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tags Stage=Test,CostCenter=80432,Owner=SysEng
```

Affichage des balises

Utilisez les commandes suivantes pour afficher les balises que vous avez attribuées à votre ensemble d'autorisations.

Example **`list-tags-for-resource`**Commande pour un ensemble d'autorisations

Affichez les balises attribuées à un ensemble d'autorisations à l'aide `list-tags-for-resource`de l'`sso`ensemble de commandes :

```
$ aws sso-admin list-tags-for-resource --resource-arn sso-resource-arn
```

Suppression de balises

Utilisez les commandes suivantes pour supprimer des balises d'un ensemble d'autorisations.

Example **`untag-resource`**Commande pour un ensemble d'autorisations

Supprimez les balises d'un ensemble d'autorisations en utilisant `untag-resource`dans le `sso` jeu de commandes :

```
$ aws sso-admin untag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tag-keys Stage CostCenter Owner
```

Pour le paramètre `--tag-keys`, spécifiez une ou plusieurs clés de balise et n'incluez pas les valeurs de balise.

Appliquer des balises lors de la création d'un ensemble d'autorisations

Utilisez les commandes suivantes pour attribuer des balises au moment de créer un ensemble d'autorisations.

Example Commande **`create-permission-set`** avec des identifications

Lorsque vous créez un ensemble d'autorisations à l'aide de la `create-permission-set`commande, vous pouvez spécifier des balises avec le `--tags` paramètre suivant :

```
$ aws sso-admin create-permission-set \
> --instance-arn sso-instance-arn \
> --name permission=set-name \
> --tags Stage=Test,CostCenter=80432,Owner=SysEng
```

Gérez les balises à l'aide de l'API IAM Identity Center

Vous pouvez utiliser les actions suivantes dans l'API IAM Identity Center pour gérer les balises associées à votre ensemble d'autorisations.

Actions d'API pour les balises d'instance IAM Identity Center

Utilisez les actions d'API suivantes pour attribuer, afficher et supprimer des balises pour un ensemble d'autorisations ou une instance d'IAM Identity Center.

- TagResource
- ListTagsForResource
- UntagResource
- CreatePermissionSet
- CreateInstance

Intégration d'AWSCLI avec IAM Identity Center

AWSL'intégration de l'interface de ligne de commande (CLI) version 2 avec IAM Identity Center simplifie le processus de connexion. Les développeurs peuvent se connecter directement auAWS CLIen utilisant les mêmes informations d'identification Active Directory ou IAM Identity Center que celles qu'ils utilisent normalement pour se connecter à IAM Identity Center et accéder aux comptes et rôles qui leur sont attribués. Par exemple, une fois qu'un administrateur a configuré IAM Identity Center pour utiliser Active Directory pour l'authentification, un développeur peut se connecter auAWS CLIdirectement avec leurs informations d'identification Active Directory.

AWSL'intégration de la CLI avec IAM Identity Center offre les avantages suivants :

- Les entreprises peuvent permettre à leurs développeurs de se connecter à l'aide des informations d'identification d'IAM Identity Center ou d'Active Directory en connectant IAM Identity Center à leur Active Directory à l'aide deAWS Directory Service.
- Les développeurs peuvent se connecter à partir de la CLI pour un accès plus rapide.
- Les développeurs peuvent répertorier et basculer entre les comptes et les rôles auxquels ils ont accès.
- Les développeurs peuvent générer et enregistrer automatiquement des profils de rôle nommés dans leur configuration CLI et les référencer dans l'interface de ligne de commande pour exécuter des commandes dans les comptes et les rôles souhaités.
- La CLI gère automatiquement les informations d'identification à court terme afin que les développeurs puissent démarrer et rester dans la CLI en toute sécurité, sans interruption, et exécuter des scripts de longue durée.

Fonctionnement de l'intégration avecAWSCLI avec IAM Identity Center

Pour utiliser le pluginAWSIntégration de l'interface de ligne de commande avec IAM Identity Center, vous devez télécharger, installer et configurerAWS Command Line Interfaceversion 2. Pour obtenir des instructions détaillées sur la façon de télécharger et d'intégrer leAWS CLIavec IAM Identity Center, consultezConfiguration deAWSCLI pour utiliser IAM Identity Centerdans leAWS Command Line InterfaceGuide de l'utilisateur.

AWS IAM Identity Center Disponibilité de la région

IAM Identity Center est disponible dans plusieurs versions couramment utilisées Régions AWS. Cette disponibilité vous permet de configurer plus facilement l'accès des utilisateurs à Comptes AWS de multiples applications professionnelles. Lorsque vos utilisateurs se connectent au portail AWS d'accès, ils peuvent sélectionner celui Compte AWS pour lequel ils sont autorisés, puis accéder au AWS Management Console. Pour obtenir la Régions AWS liste complète des solutions prises en charge par IAM Identity Center, consultez la section Points de terminaison et quotas d'IAM Identity Center.

Données de la région du centre d'identité IAM

Lorsque vous activez IAM Identity Center pour la première fois, toutes les données que vous configurez dans IAM Identity Center sont stockées dans la région où vous les avez configurées. Ces données incluent les configurations d'annuaires, les ensembles d'autorisations, les instances d'applications et les affectations d'utilisateurs aux Compte AWS applications. Si vous utilisez le magasin d'identités IAM Identity Center, tous les utilisateurs et groupes que vous créez dans IAM Identity Center sont également stockés dans la même région. Nous vous recommandons d'installer IAM Identity Center dans une région que vous souhaitez garder disponible pour les utilisateurs, et non dans une région que vous devrez peut-être désactiver.

AWS Organizations n'en prend en charge qu'un seul Région AWS à la fois. Pour activer IAM Identity Center dans une autre région, vous devez d'abord supprimer votre configuration IAM Identity Center actuelle. Le passage à une autre région modifie également l'URL du portail AWS d'accès, et vous devez reconfigurer tous les ensembles d'autorisations et les attributions.

Appels interrégionaux

IAM Identity Center utilise Amazon Simple Email Service (Amazon SES) pour envoyer des e-mails aux utilisateurs finaux lorsqu'ils tentent de se connecter avec un mot de passe à usage unique (OTP) comme deuxième facteur d'authentification. Ces e-mails sont également envoyés pour certains événements de gestion de l'identité et des informations d'identification, par exemple lorsque l'utilisateur est invité à configurer un mot de passe initial, à vérifier une adresse e-mail et à réinitialiser son mot de passe. Amazon SES est disponible dans un sous-ensemble de Régions AWS ceux pris en charge par IAM Identity Center.

IAM Identity Center appelle les points de terminaison locaux d'Amazon SES lorsqu'Amazon SES est disponible localement dans un. Région AWS Lorsqu'Amazon SES n'est pas disponible localement,

IAM Identity Center appelle les points de terminaison Amazon SES d'une autre manière Région AWS, comme indiqué dans le tableau suivant.

Les codes de région Amazon SES sont répertoriés dans le tableau suivant.

Code de région du centre d'identité IAM	Nom de la région du centre d'identité IAM	Code de région Amazon SES	Nom de la région Amazon SES
us-gov-east-1	AWS GovCloud (USA Est)	us-gov-west-1	AWS GovCloud (US-Ouest)
ap-east-1	Asie-Pacifique (Hong Kong)	ap-northeast-2	Asie-Pacifique (Séoul)
ap-southeast-4	Asie-Pacifique (Melbourne)	ap-southeast-2	Asie-Pacifique (Sydney)
ap-south-2	Asie-Pacifique (Hyderabad)	ap-south-1	Asie-Pacifique (Mumbai)
eu-central-2	Europe (Zurich)	eu-central-1	Europe (Francfort)
eu-south-2	Europe (Espagne)	eu-west-3	Europe (Paris)
me-central-1	Moyen-Orient (EAU)	eu-central-1	Europe (Francfort)

Lors de ces appels interrégionaux, IAM Identity Center peut envoyer les attributs utilisateur suivants :

- Adresse e-mail
- Prénom
- Nom
- Compte dans AWS Organizations
- AWS URL du portail d'accès
- Nom d'utilisateur
- ID de l'annuaire
- ID de l'utilisateur

Gestion du centre d'identité IAM dans une région optionnelle (région désactivée par défaut)

La plupart Régions AWS sont activés par défaut pour les opérations dans tous les AWS services. Celles Les régions sont automatiquement activées pour être utilisées avec IAM Identity Center. Les régions suivantes Régions AWS sont facultatives et vous devez les activer :

- Afrique (Le Cap)
- Asie-Pacifique (Hong Kong)
- Asie-Pacifique (Jakarta)
- Asie-Pacifique (Melbourne)
- Asie-Pacifique (Hyderabad)
- Europe (Milan)
- Europe (Zurich)
- Europe (Espagne)
- Israël (Tel Aviv)
- Moyen-Orient (Bahreïn)
- Moyen-Orient (EAU)

Lorsque vous activez IAM Identity Center pour un compte de gestion dans le cadre d'un opt-in Région AWS, les métadonnées IAM Identity Center suivantes pour tous les comptes membres sont stockées dans la région.

- ID de compte
- Nom du compte
- Adresse e-mail du compte
- Amazon Resource Names (ARN) des rôles IAM créés par IAM Identity Center dans le compte membre

Si vous désactivez une région dans laquelle IAM Identity Center est installé, IAM Identity Center est également désactivé. Une fois le centre d'identité IAM désactivé dans une région, les utilisateurs de cette région ne pourront plus accéder aux Comptes AWS applications par authentification unique. AWS conserve les données de votre configuration IAM Identity Center pendant au moins 10 jours. Si

vous réactivez IAM Identity Center dans ce délai, les données de configuration de votre IAM Identity Center seront toujours disponibles dans la région.

Pour réactiver IAM Identity Center en mode opt-in Régions AWS, vous devez réactiver la région. Comme IAM Identity Center doit à nouveau traiter tous les événements suspendus, la réactivation d'IAM Identity Center peut prendre un certain temps.

> **Note**
>
> IAM Identity Center peut gérer l'accès uniquement à ceux Comptes AWS qui sont activés pour une utilisation dans un Région AWS. Pour gérer l'accès à tous les comptes de votre organisation, activez IAM Identity Center dans le compte de gestion Région AWS qui est automatiquement activé pour être utilisé avec IAM Identity Center.

Pour plus d'informations sur l'activation et la désactivation Régions AWS, consultez la section Gestion Régions AWS dans le manuel de référence AWS général.

Supprimer la configuration de votre IAM Identity Center

Lorsqu'une configuration IAM Identity Center est supprimée, toutes les données de cette configuration sont supprimées et ne peuvent pas être récupérées. Le tableau suivant décrit les données supprimées en fonction du type de répertoire actuellement configuré dans IAM Identity Center.

Quelles données sont supprimées	Répertoire connecté (AWS Managed Microsoft AD ou AD Connector)	Boutique d'identités IAM Identity Center
Tous les ensembles d'autorisations que vous avez configurés pour Comptes AWS	✓	✓
Toutes les applications que vous avez configurées dans IAM Identity Center	✓	✓

Quelles données sont supprimées	Répertoire connecté (AWS Managed Microsoft AD ou AD Connector)	Boutique d'identités IAM Identity Center
Toutes les attributions d'utilisateurs que vous avez configurées Comptes AWS et les applications	✓	✓
Tous les utilisateurs et groupes de l'annuaire ou du magasin	S/O	✓

Utilisez la procédure suivante lorsque vous devez supprimer la configuration actuelle de votre IAM Identity Center.

Pour supprimer la configuration de votre IAM Identity Center

1. Ouvrez la console IAM Identity Center.
2. Dans le panneau de navigation de gauche, choisissez Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Gestion.
4. Dans la section Supprimer la configuration du centre d'identité IAM, choisissez Supprimer.
5. Dans la boîte de dialogue de configuration Supprimer IAM Identity Center, cochez chacune des cases pour confirmer que vous comprenez que vos données seront supprimées. Tapez votre instance IAM Identity Center dans la zone de texte, puis choisissez Confirmer.

AWS IAM Identity Center quotas

Les tableaux suivants décrivent les quotas au sein d'IAM Identity Center. Les demandes d'augmentation de quota doivent provenir d'un compte de gestion ou d'un compte d'administrateur délégué. Pour augmenter un quota, voir Demande d'augmentation de quota.

> **Note**
>
> Nous vous recommandons d'utiliser la AWS CLI et les API si vous avez plus de 50 000 utilisateurs, 10 000 groupes ou 500 ensembles d'autorisations. Pour plus d'informations sur la CLI, consultezIntégration d'AWSCLI avec IAM Identity Center. Pour plus d'informations sur les API, consultez la section Welcome to the IAM Identity Center API Reference.

Quotas de candidatures

Ressource	Quota par défaut	Peut être augmenté
Taille du fichier de certificats SAML du fournisseur de services (au format PEM)	2 Ko	Non
Limite d'assertion SAML	50 000 caractères	Non
Limite de taille de fichier du certificat IdP téléchargé vers IAM Identity Center	2500 caractères (UTF-8)	Non
Étendue d'accès par application	25	Non

Compte AWS quotas

Ressource	Quota par défaut	Peut être augmenté
Nombre d'ensembles d'autorisations autorisés dans IAM Identity Center	2000	Oui
Nombre d'ensembles d'autorisations fournis autorisés par Compte AWS	250	Oui
Nombre de stratégies en ligne par jeu d'autorisations	1	Non
Nombre de politiques AWS gérées et gérées par le client par ensemble d'autorisations	20 [1]	Non
Taille maximale de stratégie en ligne par jeu d'autorisations	32 768 octets. La taille maximale des caractères autres que des espaces blancs dans la politique intégrée par ensemble d'autorisations est de 10 240 octets.	Non
Nombre de rôles IAM (ensembles d'autorisations) dans le Compte AWS qui peuvent être mis à jour à la fois	1	Non

[1]AWS Identity and Access Management (IAM) définit un quota de 10 politiques gérées par rôle. Pour tirer parti de ce quota, demandez une augmentation du quota IAM. Politiques gérées associées à

un rôle IAM dans la console Service Quotas pour chaque Compte AWS endroit où vous souhaitez déployer l'ensemble d'autorisations.

> **Note**
>
> Jeux d'autorisationssont fournis en Comptes AWS tant que rôles IAM, ou utilisent des rôles IAM existants dans Comptes AWS, et respectent donc les quotas IAM. Pour plus d'informations sur les quotas associés aux rôles IAM, consultez la section Quotas IAM et STS.

Quotas Active Directory

Ressource	Quota par défaut	Peut être augmenté
Nombre d'annuaires connectés que vous pouvez avoir simultanément	1	Non

Quotas de banque d'identités IAM Identity Center

Ressource	Quota par défaut	Peut être augmenté
Nombre d'utilisateurs pris en charge dans IAM Identity Center	100 000	Oui
Nombre de groupes pris en charge dans IAM Identity Center	100 000	Non
Nombre de groupes uniques pouvant être utilisés pour évaluer les autorisations d'un utilisateur	1 000	Non

Limites de limitation de l'IAM Identity Center

Ressource	Quota par défaut
API du centre d'identité IAM	Les API IAM Identity Center ont un accélérateur collectif maximal de 20 transactions par seconde (TPS). Le CreateAccountAssignmenttaux maximum d'appels asynchrones en attente est de 10. Ces quotas ne peuvent pas être modifiés.

Quotas supplémentaires

Ressource	Quota par défaut	Peut être augmenté
Nombre total Comptes AWS d'applications pouvant être configurées*	3000	Oui
Nombre total d'instances d'IAM Identity Center par compte	1	Non
Nombre total d'émetteurs de jetons fiables	10	Non

* Jusqu'à 3 000 Comptes AWS applications (total combiné) sont prises en charge. Par exemple, vous pouvez configurer 2 750 comptes et 250 applications, soit un total de 3 000 comptes et applications.

Résolution des problèmes liés à IAM Identity Center

Les informations suivantes peuvent vous aider à résoudre certains problèmes courants que vous pouvez rencontrer lors de la configuration ou de l'utilisation de la console IAM Identity Center.

Problèmes lors de la création d'une instance de compte d'IAM Identity Center

Plusieurs restrictions peuvent s'appliquer lors de la création d'une instance de compte d'IAM Identity Center. Si vous ne parvenez pas à créer une instance de compte via la console IAM Identity Center ou via l'expérience de configuration d'une application AWS gérée prise en charge, vérifiez les cas d'utilisation suivants :

- Régions AWS Cochez la case autre Compte AWS dans laquelle vous essayez de créer l'instance de compte. Vous êtes limité à une instance d'IAM Identity Center par. Compte AWS Pour activer l'application, passez à l'instance Région AWS avec IAM Identity Center ou passez à un compte sans instance d'IAM Identity Center.
- Si votre organisation a activé IAM Identity Center avant le 14 septembre 2023, votre administrateur devra peut-être accepter la création d'une instance de compte. Collaborez avec votre administrateur pour activer la création d'instances de compte à partir de la console IAM Identity Center dans le compte de gestion.
- Votre administrateur a peut-être créé une politique de contrôle des services pour limiter la création d'instances de compte d'IAM Identity Center. Travaillez avec votre administrateur pour ajouter votre compte à la liste des autorisations.

Vous recevez un message d'erreur lorsque vous tentez d'afficher la liste des applications cloud préconfigurées pour fonctionner avec IAM Identity Center

L'erreur suivante se produit lorsque vous avez une politique qui autorise les autres API IAM Identity Center, `sso:ListApplications` mais pas les autres. Mettez à jour votre politique pour corriger cette erreur.

L'`ListApplications`autorisation autorise plusieurs API :

- L'`ListApplications`API.
- API interne similaire à l'`ListApplicationProviders`API utilisée dans la console IAM Identity Center.

Pour aider à résoudre le problème de duplication, l'API interne autorise désormais également l'utilisation de l'`ListApplicationProviders`action. Pour autoriser l'`ListApplications`API publique mais refuser l'API interne, votre politique doit inclure une déclaration refusant l'`ListApplicationProviders`action :

```
      "Statement": [
    {
         "Effect": "Deny",
         "Action": "ListApplicationProviders",
         "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": "ListApplications",
        "Resource": "<instanceArn>" // (or "*" for all instances)
    }
]
```

Pour autoriser l'API interne mais la refuser`ListApplications`, la politique doit uniquement autoriser`ListApplicationProviders`. L'`ListApplications`API est refusée si elle n'est pas explicitement autorisée.

```
      "Statement": [
    {
         "Effect": "Allow",
         "Action": "ListApplicationProviders",
         "Resource": "*"
    }
]
```

Lorsque vos politiques sont mises à jour, contactez-nous AWS Support pour que cette mesure proactive soit supprimée.

Problèmes relatifs au contenu des assertions SAML créées par IAM Identity Center

IAM Identity Center fournit une expérience de débogage basée sur le Web pour les assertions SAML créées et envoyées par IAM Identity Center, y compris les attributs contenus dans ces assertions, lors de l'accès, Comptes AWS et pour les applications SAML depuis le portail d'accès. AWS Pour voir les détails d'une assertion SAML générée par IAM Identity Center, procédez comme suit.

1. Connectez-vous au portail d' AWS accès.
2. Lorsque vous êtes connecté au portail, maintenez la touche Shift enfoncée, choisissez la vignette de l'application, puis relâchez la touche Shift.
3. Examinez les informations indiquées sur la page intitulée You are now in administrator mode (Vous êtes maintenant en mode administrateur). Pour conserver ces informations pour référence future, choisissez Copier le code XML et collez le contenu ailleurs.
4. Choisissez Envoyer pour <application>continuer. Cette option envoie l'assertion au fournisseur de services.

> **Note**
>
> Certaines configurations de navigateur et certains systèmes d'exploitation peuvent ne pas prendre en charge cette procédure. Cette procédure a été testée sur Windows 10 à l'aide des navigateurs Firefox, Chrome et Edge.

Des utilisateurs spécifiques ne parviennent pas à se synchroniser avec IAM Identity Center à partir d'un fournisseur SCIM externe

Si la synchronisation SCIM réussit pour un sous-ensemble d'utilisateurs configuré dans votre IdP pour le provisionnement dans IAM Identity Center, mais échoue pour d'autres utilisateurs, il se peut qu'une erreur similaire à celle de votre fournisseur d'identité s'affiche. `'Request is unparsable, syntactically incorrect, or violates schema'` Vous pouvez également voir des messages d'échec de provisionnement détaillés dans AWS CloudTrail.

Ce problème indique souvent que l'utilisateur de votre IdP est configuré d'une manière qui n'est pas prise en charge par IAM Identity Center. Tous les détails de la mise en œuvre du SCIM d'IAM Identity

Center, y compris les spécifications des paramètres et opérations obligatoires, facultatifs et interdits pour les objets utilisateur, sont disponibles dans le guide du développeur de mise en œuvre d'IAM Identity Center SCIM. Le guide du développeur SCIM doit être considéré comme faisant autorité en ce qui concerne les informations relatives aux exigences du SCIM. Cependant, voici quelques raisons courantes à l'origine de cette erreur :

1. L'objet utilisateur dans l'IdP n'a pas de prénom, de nom de famille et/ou de nom d'affichage.

   - Solution : ajoutez un premier (donné), un dernier (famille) et un nom d'affichage pour l'objet utilisateur. En outre, assurez-vous que les mappages de provisionnement SCIM pour les objets utilisateur de votre IdP sont configurés pour envoyer des valeurs non vides pour tous ces attributs.

2. Plusieurs valeurs pour un seul attribut sont envoyées à l'utilisateur (également appelées « attributs à valeurs multiples »). Par exemple, l'utilisateur peut avoir un numéro de téléphone professionnel et un numéro de téléphone personnel spécifiés dans l'IdP, ou plusieurs adresses électroniques ou physiques, et votre IdP est configuré pour essayer de synchroniser plusieurs ou toutes les valeurs pour cet attribut.

   - Options de solution :

     i. Mettez à jour vos mappages de provisionnement SCIM pour les objets utilisateur de votre IdP afin de n'envoyer qu'une seule valeur pour un attribut donné. Par exemple, configurez un mappage qui envoie uniquement le numéro de téléphone professionnel de chaque utilisateur.

     ii. Si les attributs supplémentaires peuvent être supprimés en toute sécurité de l'objet utilisateur au niveau de l'IdP, vous pouvez supprimer les valeurs supplémentaires, en laissant une ou zéro valeur définie pour cet attribut pour l'utilisateur.

     iii. Si l'attribut n'est pas nécessaire pour effectuer des actions dans AWS, supprimez le mappage correspondant à cet attribut des mappages de provisionnement SCIM pour les objets utilisateur de votre IdP.

3. Votre IdP essaie de faire correspondre les utilisateurs de la cible (IAM Identity Center, dans ce cas) en fonction de plusieurs attributs. Étant donné que l'unicité des noms d'utilisateur est garantie au sein d'une instance IAM Identity Center donnée, il vous suffit de spécifier `username` l'attribut utilisé pour la mise en correspondance.

   - Solution : Assurez-vous que la configuration SCIM de votre IdP n'utilise qu'un seul attribut pour correspondre aux utilisateurs d'IAM Identity Center. Par exemple, le

mappage `username` de l'IdP à l'`userName`attribut dans SCIM pour le provisionnement vers IAM Identity Center sera correct et suffisant pour la plupart des implémentations. `userPrincipalName`

Les utilisateurs ne peuvent pas se connecter lorsque leur nom d'utilisateur est au format UPN

Les utilisateurs peuvent ne pas être en mesure de se connecter au portail AWS d'accès en fonction du format qu'ils utilisent pour saisir leur nom d'utilisateur sur la page de connexion. Dans la plupart des cas, les utilisateurs peuvent se connecter au portail utilisateur en utilisant leur nom d'utilisateur simple, leur nom de connexion de bas niveau (DOMAIN \UserName) ou leur nom de connexion UPN (). `UserName@Corp.Example.com` L'exception à cette règle est lorsque IAM Identity Center utilise un répertoire connecté qui a été activé avec la MFA et que le mode de vérification a été défini sur Context-aware ou Always-on. Dans ce scénario, les utilisateurs doivent se connecter avec leur nom de connexion de bas niveau (DOMAIN \). UserName Pour plus d'informations, consultez Authentification multifactorielle pour les utilisateurs d'Identity Center. Pour obtenir des informations générales sur les formats de nom d'utilisateur utilisés pour se connecter à Active Directory, consultez la section Formats de nom d'utilisateur sur le site Web de documentation Microsoft.

Je reçois le message d'erreur « Impossible d'effectuer l'opération sur le rôle protégé » lors de la modification d'un rôle IAM

Lorsque vous passez en revue les rôles IAM dans un compte, vous remarquerez peut-être que les noms de rôles commencent par « AWSReservedSSO _ ». Il s'agit des rôles que le service IAM Identity Center a créés dans le compte, et ils proviennent de l'attribution d'un ensemble d'autorisations au compte. Toute tentative de modification de ces rôles depuis la console IAM entraînera l'erreur suivante :

```
'Cannot perform the operation on the protected role 'AWSReservedSSO_RoleName_Here' -
 this role is only modifiable by AWS'
```

Ces rôles ne peuvent être modifiés qu'à partir de la console IAM Identity Center Administrator, qui se trouve dans le compte de gestion de AWS Organizations. Une fois les modifications apportées, vous pouvez les transférer aux AWS comptes auxquels elles sont attribuées.

Les utilisateurs de l'annuaire ne peuvent pas réinitialiser leur mot de passe

Lorsqu'un utilisateur de l'annuaire réinitialise son mot de passe à l'aide du champ Mot de passe oublié ? option lors de la connexion au portail d' AWS accès, leur nouveau mot de passe doit respecter la politique de mot de passe par défaut décrite dansExigences relatives aux mots de passe lors de la gestion des identités dans IAM Identity Center.

Si un utilisateur saisit un mot de passe conforme à la politique puis reçoit le message d'erreur`We couldn't update your password`, vérifiez s'il AWS CloudTrail a enregistré l'échec. Cela peut être fait en effectuant une recherche dans la console de l'historique des événements CloudTrail ou en utilisant le filtre suivant :

```
"UpdatePassword"
```

Si le message indique ce qui suit, vous devrez peut-être contacter le support :

```
"errorCode": "InternalFailure",
      "errorMessage": "An unknown error occurred“
```

Une autre cause possible de ce problème réside dans la convention de dénomination qui a été appliquée à la valeur du nom d'utilisateur. Les conventions de dénomination doivent suivre des modèles spécifiques tels que « surname.givenname ». Cependant, certains noms d'utilisateur peuvent être assez longs ou contenir des caractères spéciaux, ce qui peut entraîner la suppression de caractères dans l'appel d'API, entraînant ainsi une erreur. Vous pouvez essayer de réinitialiser le mot de passe avec un utilisateur de test de la même manière pour vérifier si tel est le cas.

Si le problème persiste, contactez le AWS Support Center.

Mon utilisateur est référencé dans un ensemble d'autorisations mais ne peut pas accéder aux comptes ou applications assignés

Ce problème peut se produire si vous utilisez le système de gestion des identités interdomaines (SCIM) pour le provisionnement automatique avec un fournisseur d'identité externe. Plus précisément, lorsqu'un utilisateur, ou le groupe dont il était membre, est supprimé puis recréé en utilisant le même nom d'utilisateur (pour les utilisateurs) ou le même nom (pour les groupes) dans le fournisseur d'identité, un nouvel identifiant interne unique est créé pour le nouvel utilisateur ou le

nouveau groupe dans IAM Identity Center. Cependant, IAM Identity Center possède toujours une référence à l'ancien identifiant dans sa base de données d'autorisations, de sorte que le nom de l'utilisateur ou du groupe apparaît toujours dans l'interface utilisateur, mais l'accès échoue. Cela est dû au fait que l'ID d'utilisateur ou de groupe sous-jacent auquel l'interface utilisateur fait référence n'existe plus.

Dans ce cas, pour rétablir l' Compte AWS accès, vous pouvez supprimer l'accès de l'ancien utilisateur ou du Compte AWS groupe auquel il a été attribué à l'origine, puis réattribuer l'accès à l'utilisateur ou au groupe. Cela met à jour l'ensemble d'autorisations avec l'identifiant correct pour le nouvel utilisateur ou le nouveau groupe. De même, pour rétablir l'accès à une application, vous pouvez supprimer l'accès de l'utilisateur ou du groupe de la liste des utilisateurs assignés à cette application, puis ajouter à nouveau l'utilisateur ou le groupe.

Vous pouvez également vérifier si l'échec AWS CloudTrail a été enregistré en recherchant dans vos CloudTrail journaux les événements de synchronisation SCIM faisant référence au nom de l'utilisateur ou du groupe en question.

Je n'arrive pas à configurer correctement mon application à partir du catalogue d'applications

Si vous avez ajouté une application depuis le catalogue d'applications d'IAM Identity Center, sachez que chaque fournisseur de services fournit sa propre documentation détaillée. Vous pouvez accéder à ces informations depuis l'onglet Configuration de l'application dans la console IAM Identity Center.

Si le problème est lié à la configuration de la confiance entre l'application du fournisseur de services et IAM Identity Center, assurez-vous de consulter le manuel d'instructions pour connaître les étapes de dépannage.

Erreur « Une erreur inattendue s'est produite » lorsqu'un utilisateur tente de se connecter à l'aide d'un fournisseur d'identité externe

Cette erreur peut se produire pour plusieurs raisons, mais l'une des raisons les plus courantes est une incohérence entre les informations utilisateur contenues dans la demande SAML et les informations relatives à l'utilisateur dans IAM Identity Center.

Pour qu'un utilisateur d'IAM Identity Center puisse se connecter correctement lorsqu'il utilise un IdP externe comme source d'identité, les conditions suivantes doivent être remplies :

- Le format SAML NameID (configuré chez votre fournisseur d'identité) doit être « e-mail »
- La valeur NameID doit être une chaîne correctement formatée (RFC2822) (user@domain.com)
- La valeur NameID doit correspondre exactement au nom d'utilisateur d'un utilisateur existant dans IAM Identity Center (peu importe que l'adresse e-mail dans IAM Identity Center corresponde ou non, la correspondance entrante est basée sur le nom d'utilisateur)
- L'implémentation de la fédération SAML 2.0 par IAM Identity Center ne prend en charge qu'une seule assertion dans la réponse SAML entre le fournisseur d'identité et IAM Identity Center. Il ne prend pas en charge les assertions SAML chiffrées.
- Les instructions suivantes s'appliquent si cette option Attributs pour le contrôle d'accès est activée dans votre compte IAM Identity Center :
  - Le nombre d'attributs mappés dans la demande SAML doit être inférieur ou égal à 50.
  - La demande SAML ne doit pas contenir d'attributs à valeurs multiples.
  - La demande SAML ne doit pas contenir plusieurs attributs portant le même nom.
  - L'attribut ne doit pas contenir de XML structuré comme valeur.
  - Le format du nom doit être un format spécifié par SAML et non un format générique.

> **Note**
>
> IAM Identity Center n'effectue pas de création « juste à temps » d'utilisateurs ou de groupes pour les nouveaux utilisateurs ou groupes via la fédération SAML. Cela signifie que l'utilisateur doit être précréé dans IAM Identity Center, soit manuellement, soit via un provisionnement automatique, afin de se connecter à IAM Identity Center.

Cette erreur peut également se produire lorsque le point de terminaison Assertion Consumer Service (ACS) configuré dans votre fournisseur d'identité ne correspond pas à l'URL ACS fournie par votre instance IAM Identity Center. Assurez-vous que ces deux valeurs correspondent exactement.

En outre, vous pouvez résoudre les problèmes de connexion à un fournisseur d'identité externe en accédant au nom ExternalId de l'événement AWS CloudTrail P et en filtrant sur celui-ci. DirectoryLogin

Erreur « Impossible d'activer les attributs du contrôle d'accès »

Cette erreur peut se produire si l'utilisateur qui active ABAC ne dispose pas des `iam:UpdateAssumeRolePolicy` autorisations requises pour l'activerAttributs pour le contrôle d'accès.

Je reçois un message « Navigateur non pris en charge » lorsque je tente d'enregistrer un appareil pour le MFA

WebAuthn est actuellement compatible avec les navigateurs Web Google Chrome, Mozilla Firefox, Microsoft Edge et Apple Safari, ainsi que sur les plateformes Windows 10 et Android. Certains éléments de WebAuthn prise en charge peuvent varier, tels que la prise en charge de l'authentificateur de plateforme sur les navigateurs macOS et iOS. Si les utilisateurs tentent d'enregistrer des WebAuthn appareils sur un navigateur ou une plateforme non pris en charge, certaines options non prises en charge seront grisées, ou ils recevront un message d'erreur indiquant que toutes les méthodes prises en charge ne sont pas prises en charge. Dans ces cas, reportez-vous à FIDO2 : Web Authentication (WebAuthn) pour plus d'informations sur la prise en charge du navigateur/de la plateforme. Pour plus d'informations sur WebAuthn IAM Identity Center, consultezAuthentificateurs FIDO2.

Le groupe « Utilisateurs du domaine » Active Directory ne se synchronise pas correctement avec IAM Identity Center

Le groupe d'utilisateurs du domaine Active Directory est le « groupe principal » par défaut pour les objets utilisateur AD. Les groupes principaux Active Directory et leurs adhésions ne peuvent pas être lus par IAM Identity Center. Lorsque vous attribuez l'accès aux ressources ou aux applications IAM Identity Center, utilisez des groupes autres que le groupe des utilisateurs du domaine (ou d'autres groupes assignés en tant que groupes principaux) pour que l'appartenance au groupe soit correctement reflétée dans la banque d'identités IAM Identity Center.

Erreur d'identification MFA non valide

Cette erreur peut se produire lorsqu'un utilisateur tente de se connecter à IAM Identity Center à l'aide d'un compte fourni par un fournisseur d'identité externe (par exemple, Okta ouMicrosoft Entra ID) avant que son compte ne soit entièrement provisionné auprès d'IAM Identity Center à l'aide du protocole SCIM. Une fois le compte utilisateur configuré auprès d'IAM Identity Center, ce problème

doit être résolu. Vérifiez que le compte a été fourni à IAM Identity Center. Dans le cas contraire, consultez les journaux de provisionnement dans le fournisseur d'identité externe.

Je reçois un message « Une erreur inattendue s'est produite » lorsque je tente de m'inscrire ou de me connecter à l'aide d'une application d'authentification

Les systèmes de mot de passe à usage unique basé sur le temps (TOTP), tels que ceux utilisés par IAM Identity Center en combinaison avec des applications d'authentification basées sur du code, reposent sur la synchronisation de l'heure entre le client et le serveur. Assurez-vous que l'appareil sur lequel votre application d'authentification est installée est correctement synchronisé avec une source horaire fiable, ou réglez manuellement l'heure sur votre appareil pour qu'elle corresponde à une source fiable, telle que le NIST (https://www.time.gov/) ou d'autres équivalents locaux/régionaux.

Je reçois un message d'erreur « Ce n'est pas toi, c'est nous » lorsque j'essaie de me connecter à IAM Identity Center

Cette erreur indique qu'il existe un problème de configuration avec votre instance d'IAM Identity Center ou avec le fournisseur d'identité externe (IdP) qu'IAM Identity Center utilise comme source d'identité. Nous vous recommandons de vérifier les points suivants :

- Vérifiez les paramètres de date et d'heure sur l'appareil que vous utilisez pour vous connecter. Nous vous recommandons de définir la date et l'heure à régler automatiquement. Si ce n'est pas le cas, nous vous recommandons de synchroniser la date et l'heure avec un serveur NTP (Network Time Protocol) connu.
- Vérifiez que le certificat IdP téléchargé vers IAM Identity Center est le même que celui fourni par votre IdP. Vous pouvez vérifier le certificat depuis la console IAM Identity Center en accédant aux paramètres. Dans l'onglet Source d'identité, sélectionnez Action, puis sélectionnez Gérer l'authentification. Si les certificats IdP et IAM Identity Center ne correspondent pas, importez un nouveau certificat dans IAM Identity Center.
- Assurez-vous que le format NameID du fichier de métadonnées de votre fournisseur d'identité est le suivant :
  - `urn:oasis:name:tc:SAML:1.1:nameid-format:emailAddress`
- Si vous utilisez AD Connector from AWS Directory Service comme fournisseur d'identité, vérifiez que les informations d'identification du compte de service sont correctes et n'ont pas expiré.

Consultez Mettre à jour les informations d'identification de votre compte de service AD Connector AWS Directory Service pour plus d'informations.

Mes utilisateurs ne reçoivent pas d'e-mails d'IAM Identity Center

Tous les e-mails envoyés par le service IAM Identity Center proviendront soit de l'adresse`no-reply@signin.aws`, soit de. `no-reply@login.awsapps.com` Votre système de messagerie doit être configuré de manière à accepter les e-mails provenant de ces adresses électroniques d'expéditeurs et à ne pas les traiter comme du courrier indésirable ou du spam.

Erreur : vous ne pouvez pas supprimer/modifier/supprimer/attribuer l'accès aux ensembles d'autorisations fournis dans le compte de gestion

Ce message indique que la Administration déléguée fonctionnalité a été activée et que l'opération que vous avez tentée précédemment ne peut être exécutée avec succès que par une personne disposant d'autorisations de compte de gestion AWS Organizations. Pour résoudre ce problème, connectez-vous en tant qu'utilisateur disposant de ces autorisations et réessayez d'exécuter la tâche ou attribuez cette tâche à une personne disposant des autorisations appropriées. Pour plus d'informations, consultez Enregistrez un compte membre.

Erreur : jeton de session introuvable ou non valide

Cette erreur peut se produire lorsqu'un client, tel qu'un navigateur Web AWS CLI, essaie d'utiliser une session révoquée ou invalidée côté serveur. AWS Toolkit Pour résoudre ce problème, retournez sur l'application client ou sur le site Web et réessayez, y compris en vous reconnectant si vous y êtes invité. Cela peut parfois vous obliger à annuler également les demandes en attente, telles qu'une tentative de connexion en attente AWS Toolkit depuis votre IDE.

Historique du document

Le tableau suivant décrit les ajouts importants à la AWS IAM Identity Center documentation. Nous mettons aussi la documentation à jour régulièrement pour prendre en compte les commentaires qui nous sont envoyés.

- Dernière mise à jour majeure de la documentation : 23 septembre 2022

Modification	Description	Date
Mises à jour pour les politiques AWS gérées	Autorisations mises à jour pour la politique `AWSIAMIdentityCenterAllowListForIdentityContext` AWS gérée.	17 mai 2024
Mises à jour pour les politiques AWS gérées	Autorisations mises à jour pour la politique `AWSIAMIdentityCenterAllowListForIdentityContext` AWS gérée.	30 avril 2024
Mises à jour pour les politiques AWS gérées	Autorisations mises à jour pour la politique `AWSSSOMasterAccountAdministrator` AWS gérée.	26 avril 2024
Mises à jour pour les politiques AWS gérées	Autorisations mises à jour pour la politique `AWSSSOMemberAccountAdministrator` AWS gérée.	26 avril 2024
Mises à jour pour les politiques AWS gérées	Autorisations mises à jour pour la politique `AWSSSOReadOnly` AWS gérée.	26 avril 2024

Mises à jour pour les politiques AWS gérées	Autorisations mises à jour pour la politique `AWSIAMIdentityCenterAllowListForIdentityContext` AWS gérée.	26 avril 2024
Mises à jour pour les politiques AWS gérées	Autorisations mises à jour pour la politique `AWSIAMIdentityCenterAllowListForIdentityContext` AWS gérée.	24 avril 2024
Mises à jour pour les politiques AWS gérées	Autorisations mises à jour pour la politique `AWSIAMIdentityCenterAllowListForIdentityContext` AWS gérée.	19 avril 2024
Mises à jour pour les politiques AWS gérées	Autorisations mises à jour pour la politique `AWSIAMIdentityCenterAllowListForIdentityContext` AWS gérée.	11 avril 2024
Mises à jour pour les politiques AWS gérées	Autorisations mises à jour pour la politique `AWSIAMIdentityCenterAllowListForIdentityContext` AWS gérée.	26 novembre 2023
Nouveau sujet AWS relatif aux politiques gérées	Ajout de détails sur la politique `AWSIAMIdentityCenterAllowListForIdentityContext` AWS gérée.	15 novembre 2023

Conseils améliorés pour démarrer avec IAM Identity Center	Ajout de nouveau contenu pour démarrer avec IAM Identity Center et créer un utilisateur administratif	23 septembre 2022
Utilisateurs et groupes mis à jour dans la référence d'API Identity Center	Cette mise à jour inclut des références aux nouvelles API de création, de mise à jour et de suppression dans le guide de référence des API Identity Center.	31 août 2022
AWS Authentification unique (AWS SSO) renommée en AWS IAM Identity Center	AWS présente AWS IAM Identity Center. IAM Identity Center étend les fonctionn alités de AWS Identity and Access Management (IAM) pour vous aider à gérer de manière centralisée les comptes et l'accès aux applications pour les utilisate urs de votre personnel. Les fonctionnalités d'IAM Identity Center incluent les attributions d'applications, les autorisat ions multi-comptes et un portail d' AWS accès.	26 juillet 2022
Support des limites d'autoris ations et des politiques gérées par le client dans les ensembles d'autorisations	Ajout de contenu pour l'utilisa tion de politiques AWS gérées et gérées par le client AWS Identity and Access Management (IAM) avec des ensembles d'autorisations.	14 juillet 2022

Support pour les AWS régions activées manuellement	Ajout de contenu pour l'utilisation d'IAM Identity Center dans les régions activées manuellement.	15 juin 2022
Mises à jour pour les politiques AWS gérées	Autorisations mises à jour pour la politique `AWSSSOServiceRolePolicy` AWS gérée.	11 mai 2022
Support pour l'administration déléguée	Ajout de contenu pour la fonctionnalité d'administration déléguée.	11 mai 2022
Mises à jour pour les politiques AWS gérées	Autorisations mises à jour pour le `AWSSSOMasterAccountAdministrator` `AWSSSOMemberAccountAdministrator` , et les politiques `AWSSSOReadOnly` AWS gérées.	28 avril 2022
Support pour la synchronisation AD configurable	Ajout de contenu pour la fonctionnalité configurable de synchronisation AD.	14 avril 2022
Nouveau sujet AWS relatif aux politiques gérées	Ajout de détails sur la politique `AWSSSOMasterAccountAdministrator` AWS gérée.	4 août 2021
Mises à jour des quotas	Ajustements des tableaux de quotas.	21 décembre 2020

Nouveaux exemples de politiques	De nouveaux exemples de politiques gérées par le client ont été ajoutés et des mises à jour ont été apportées à la section des autorisations requises.	21 décembre 2020
Support pour le contrôle d'accès basé sur les attributs (ABAC)	Ajout de contenu pour la fonctionnalité ABAC.	24 novembre 2020
Support à l'inscription forcée au MFA	Mises à jour pour obliger les utilisateurs à inscrire un appareil MFA lors de la connexion.	23 novembre 2020
Support pour WebAuthn	Du contenu a été ajouté pour WebAuthn une nouvelle fonctionnalité.	20 novembre 2020
Support pour Ping Identity	Ajout de contenu à intégrer aux Ping Identity produits en tant que fournisseur d'identité externe pris en charge.	26 octobre 2020
Support pour OneLogin	Ajout de contenu à intégrer en OneLogin tant que fournisse ur d'identité externe pris en charge.	31 juillet 2020
Prise en charge pour Okta	Ajout de contenu à intégrer en Okta tant que fournisse ur d'identité externe pris en charge.	28 mai 2020

Support pour les fournisseurs d'identité externes	Modification des référence s du répertoire à la source d'identité, ajout de contenu pour prendre en charge les fournisseurs d'identité externes.	26 novembre 2019
Nouveaux paramètres MFA	Suppression de la rubrique de validation en deux étapes et ajout d'une nouvelle rubrique MFA à sa place.	24 octobre 2019
Nouveau paramètre pour ajouter la validation en deux étapes	Ajout de contenu expliquant comment activer la validatio n en deux étapes pour les utilisateurs.	16 janvier 2019
Support de la durée de session sur les AWS comptes	Ajout de contenu expliquant comment définir la durée de session d'un AWS compte.	30 octobre 2018
Nouvelle option pour utiliser le répertoire Identity Center	Ajout de contenu permettant de choisir le répertoire Identity Center ou de se connecter à un répertoire existant dans Active Directory.	17 octobre 2018
Support de l'état du relais et de la durée de session sur les applications	Ajout de contenu sur l'état du relais et la durée de session pour les applications.	10 octobre 2018

Support supplémentaire pour les nouvelles applications	Ajouté 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, et UserEcho au catalogue d'applications.	3 août 2018
Support pour l'accès multicompte aux comptes de gestion	Ajout de contenu expliquant comment déléguer l'accès à plusieurs comptes aux utilisateurs d'un compte de gestion.	9 juillet 2018
Support pour les nouvelles applications	Ajouté DocuSign, Keeper Security, et SugarCRM au catalogue d'applications.	16 mars 2018
Obtenir des informations d'identification temporaires pour l'accès à la CLI	Ajout d'informations sur la façon d'obtenir des informations d'identification temporaires pour exécuter AWS CLI des commandes.	le 22 février 2018
Nouveau guide	Il s'agit de la première version du guide de l'utilisateur d'IAM Identity Center.	7 décembre 2017

Glossaire AWS

Pour connaître la terminologie la plus récente d'AWS, consultez le Glossaire AWS dans la Référence Glossaire AWS.

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.