AWS Single Sign-On

Guide de l'utilisateur

AWS Single Sign-On: Guide de l'utilisateur

Table of Contents

Qu'est-ce qu'AWS Single Sign-On ?

AWS Single Sign-On est un service cloud d'authentification unique (SSO) qui permet de gérer de façon centralisée l'accès SSO à tous vos comptes et applications cloud AWS. En particulier, il permet de gérer l'accès SSO et les autorisations utilisateur dans l'ensemble de vos comptes AWS dans AWS Organizations. AWS SSO vous aide également à gérer les accès et les autorisations pour les applications logicielles tierces SaaS ainsi que les applications personnalisées qui prennent en charge le langage Security Assertion Markup Language (SAML) 2.0. AWS SSO comprend un portail utilisateur dans lequel vos utilisateurs finaux peuvent trouver et ouvrir en un seul endroit tous les comptes AWS qui leur sont attribués, toutes les applications cloud et toutes les applications personnalisées.

Fonctions de AWS SSO

AWS SSO offre les fonctions suivantes :

Intégration à AWS Organizations

AWS SSO est étroitement intégré à AWS Organizations et aux opérations d'API AWS, contrairement à d'autres solutions d'authentification unique (SSO) natives cloud. AWS SSO s'intègre de manière native à AWS Organizations énumère tous vos comptes AWS. Si vous avez organisé vos comptes en unités d'organisation (UO), ceux-ci s'affichent ainsi dans la console AWS SSO. Vous pouvez ainsi reconnaître rapidement vos comptes AWS, déployer des jeux d'autorisations communs et gérer l'accès depuis un emplacement central.

Accès SSO à vos comptes et applications cloud AWS

AWS SSO vous permet de gérer facilement l'authentification unique (SSO) dans tous vos comptes AWS, applications cloud et applications SAML 2.0 personnalisées, ceci sans scripts personnalisés ou solutions SSO tierces. Utilisez la console AWS SSO pour affecter rapidement les utilisateurs qui doivent bénéficier d'un accès en un clic aux seules applications que vous avez autorisées dans leur portail utilisateur personnalisé.

Créer et gérer des utilisateurs et des groupes dans AWS SSO

Lorsque vous activez le service pour la première fois, nous créons un annuaire par défaut pour vous dans AWS SSO. Vous pouvez utiliser cet annuaire pour gérer vos utilisateurs et vos groupes directement dans la console. Ou, si vous préférez, vous pouvez vous connecter à un annuaire AWS Managed Microsoft AD existant et gérer vos utilisateurs avec les outils de gestion Active Directory standard fournis dans Windows Server. Si vous choisissez de gérer vos utilisateurs dans AWS SSO, vous pouvez créer rapidement des utilisateurs, puis les organiser facilement en groupes, tout ceci à partir de la console.

Tirer parti de vos identités d'entreprise existantes

AWS SSO est intégré à Microsoft AD via AWS Directory Service. Cela signifie que vos employés peuvent se connecter à votre portail utilisateur AWS SSO à l'aide de leurs informations d'identification Active Directory. Pour accorder aux utilisateurs Active Directory l'accès aux comptes et applications, il vous suffit de les ajouter aux groupes Active Directory appropriés. Par exemple, vous pouvez accorder au groupe DevOps un accès SSO à vos comptes AWS de production. Les utilisateurs ajoutés au groupe DevOps se voient ensuite accorder automatiquement l'accès SSO à ces comptes AWS. Cette automatisation facilite l'intégration des nouveaux utilisateurs et permet aux utilisateurs existants d'accéder rapidement à de nouveaux comptes et de nouvelles applications.

Compatibilité avec les applications cloud couramment utilisées

AWS SSO prend en charge les applications cloud couramment utilisées, comme Salesforce, Box et Office 365. L'apport d'instructions d'intégration de ces applications permet de réduire le temps nécessaire pour les configurer pour l'authentification unique (SSO). Ces instructions servent de rampes de protection pour aider les administrateurs à configurer et dépanner ces configurations SSO. Cela élimine la nécessité pour les administrateurs de connaître les nuances de configuration de chaque application cloud.

Facilité de configuration et de surveillance de l'utilisation

Avec AWS SSO, vous pouvez activer un service SSO à haute disponibilité en seulement quelques clics. Il n'y a aucune infrastructure supplémentaire à déployer ou compte AWS à configurer. AWS SSO est une infrastructure hautement disponible et entièrement sécurisée qui s'adapte à vos besoins et ne nécessite pas de gestion de logiciel ou de matériel. AWS SSO enregistre toutes les activités de connexion dans AWS CloudTrail, et vous donne ainsi la visibilité nécessaire pour surveiller et contrôler les activités SSO à un même endroit.

Démarrez

Dans cet exercice de mise en route, vous allez activer AWS Single Sign-On, connecter votre annuaire, configurer l'authentification unique (SSO) vers vos comptes AWS, puis configurer SSO pour vos applications cloud. Bien que cela ne soit pas obligatoire, nous vous recommandons de consulter Comprendre les concepts AWS Single Sign-On clés (p. 6) avant de commencer à utiliser la console afin de vous familiariser avec les les fonctions de base et la terminologie.

Rubriques

AWS SSO Prérequis

Avant de configurer AWS SSO, vous devez :

- Commencer par configurer le service AWS Organizations et activer l'option All features (Toutes les fonctions). Pour plus d'informations sur ce paramètre, consultez Activation de toutes les fonctions de votre organisation dans le Manuel de l'utilisateur AWS Organizations.
- Vous connecter avec les informations d'identification du compte principal AWS Organizations avant de commencer à configurer AWS SSO. . Ces informations d'identification sont obligatoires pour activer AWS SSO. Pour plus d'informations, consultez Création et gestion d'une organisation AWS dans le Manuel de l'utilisateur AWS Organizations. Vous ne pouvez pas configurer AWS SSO lorsque vous êtes connecté avec les informations d'identification d'un compte membre d'une organisation.
- Avoir choisi un magasin d'annuaire pour déterminer quel groupe d'utilisateurs a un accès SSO au portail utilisateur. Si vous choisissez d'utiliser l'annuaire AWS SSO par défaut pour votre magasin d'utilisateurs, aucune tâche prérequise n'est nécessaire. L'annuaire AWS SSO est créé par défaut une fois que vous avez activé AWS SSO et il est prêt à être utilisé immédiatement. L'utilisation de ce type d'annuaire n'entraîne aucun coût. Si vous choisissez de vous connecter à un annuaire Active Directory pour votre magasin d'utilisateurs, vous devez disposer des éléments suivants :
  - Un annuaire AWS Managed Microsoft AD existant configuré dans AWS Directory Service et cet annuaire doit résider dans le compte principal de votre organisation. Vous ne pouvez connecter qu'un seul annuaire AWS Managed Microsoft AD à la fois. Cependant, vous pouvez le remplacer par un autre annuaire AWS Managed Microsoft AD ou repasser à un annuaire AWS SSO à tout moment. Pour plus d'informations, consultez Création d'un annuaire AWS Managed Microsoft AD dans le AWS Directory Service Administration Guide.
  - Un annuaire AWS Managed Microsoft AD qui doit se trouver dans la région USA Est (Virginie du Nord) (us-east-1) dans laquelle AWS SSO est également disponible. AWS SSO stocke les données d'affectation dans la même région que l'annuaire. Pour administrer AWS SSO, vous devez vous trouver dans la région us-east-1. Notez également que le portail utilisateur AWS SSO utilise la même URL d'accès que votre annuaire connecté.

Activer AWS SSO

Lorsque vous ouvrez la console AWS SSO pour la première fois, vous êtes invité à activer AWS SSO avant de pouvoir commencer à le gérer. Si vous avez déjà choisi cette option, vous pouvez ignorer

cette étape. Sinon, utilisez la procédure ci-dessous pour l'activer maintenant. Une fois activé, AWS SSO reçoit les autorisations nécessaires pour créer les rôles liés à un service IAM dans les comptes AWS de votre organisation AWS. Aucun rôle lié à un service n'est créé pour l'instant. AWS SSO crée ces rôles ultérieurement au cours du processus de configuration de l'accès SSO à vos comptes AWS (voir Configurer l'authentification unique (SSO) pour vos comptes AWS (p. 4)).

Pour activer AWS SSO

1. Connectez-vous à AWS Management Console avec les informations d'identification de votre compte principal AWS Organizations.
2. Ouvrez la console AWS SSO .
3. Choisissez Enable AWS SSO (Activer AWS SSO).
4. Si vous n'avez pas encore configuré AWS Organizations, vous serez invité à créer une organisation. Choisissez Create AWS organization (Créer une organisation AWS) pour effectuer ce processus.

Choisir votre annuaire

Le choix d'un annuaire détermine l'emplacement où AWS SSO recherche les utilisateurs et les groupes qui ont besoin d'un accès SSO. Par défaut, vous obtenez un annuaire AWS SSO pour une gestion simple et rapide des utilisateurs. Le cas échéant, vous pouvez également connecter un annuaire AWS Managed Microsoft AD à votre annuaire Active Directory sur site.

AWS SSO fournit aux utilisateurs appartenant à cet annuaire un portail utilisateur personnalisé dans lequel ils peuvent lancer facilement plusieurs comptes ou applications cloud AWS. Les utilisateurs se connectent au portail à l'aide de leurs informations d'identification d'entreprise ou des informations d'identification qu'ils configurent dans AWS SSO. Une fois qu'ils se sont connectés, ils ont accès en un clic à toutes les applications et tous les comptes AWS que vous avez autorisés précédemment.

Selon le type d'annuaire que vous essayez de configurer, vous trouverez des instructions dans les rubriques ci-dessous :

- Gérer votre annuaire AWS SSO (p. 8)
- Connexion à votre annuaire Microsoft AD (p. 11)

Pour obtenir plus d'informations sur les types d'annuaire pris en charge, consultez Gérer votre annuaire (p. 8).

Configurer l'authentification unique (SSO) pour vos comptes AWS

Dans cette étape, vous allez accorder aux utilisateurs présents dans votre annuaire un accès SSO à une ou plusieurs consoles AWS pour les comptes AWS spécifiques de votre organisation AWS. Dans leur portail utilisateur, les utilisateurs ne voient alors plus que l'icône de compte AWS (par exemple, Development) à partir de laquelle ils ont été affectés. Après avoir cliqué sur l'icône, ils peuvent choisir le rôle IAM qu'ils veulent utiliser pour se connecter à AWS Management Console pour ce compte AWS.

Pour commencer à attribuer un accès SSO à vos comptes AWS, consultez Attribution d'un accès utilisateur (p. 17).

Configurer l'authentification unique (SSO) pour vos applications cloud

Selon le type d'application que vous essayez de configurer, suivez l'une des procédures ci-dessous :

- Ajout et configuration d'une application cloud (p. 24)
- Ajout et configuration d'une application SAML 2.0 personnalisée (p. 25)

Pour obtenir plus d'informations sur les types d'application pris en charge, consultez Gestion de l'accès SSO à vos applications (p. 22).

Lorsque vous avez terminé la procédure appropriée, AWS SSO est configuré correctement, ainsi que la relation d'approbation avec votre fournisseur de services. Vos utilisateurs peuvent désormais accéder à ces applications à partir de leur portail utilisateur sur la base des autorisations que vous avez attribuées.

Comprendre les concepts AWS Single Sign-On clés

Vous tirerez mieux parti d'AWS Single Sign-On si vous vous familiarisez avec les concepts clés relatifs à la fédération SAML, à l'authentification des utilisateurs et aux autorisations IAM.

Rubriques

Fédération SAML

AWS SSO prend en charge la fédération d'identité avec SAML (Security Assertion Markup Language) 2.0. SAML 2.0 est une norme industrielle utilisée pour échanger en toute sécurité les assertions SAML qui transmettent des informations sur un utilisateur entre une autorité SAML (appelée fournisseur d'identité ou IdP). Le service AWS SSO utilise ces informations pour fournir l'authentification unique (SSO) fédérée aux utilisateurs autorisés à utiliser des applications dans le portail utilisateur AWS SSO.

AWS SSO ajoute des fonctionnalités SAML IdP à votre annuaire AWS Managed Microsoft AD ou AWS SSO. Les utilisateurs peuvent ensuite se connecter avec une authentification unique aux services qui prennent en charge SAML, notamment à AWS Management Console et aux applications tierces, par exemple Office 365, Concur et Salesforce. À l'heure actuelle, AWS SSO ne prend pas en charge d'autres types d'annuaire ou d'IdP.

Authentifications utilisateur

Lorsqu'un utilisateur se connecte au portail utilisateur à l'aide de son nom d'utilisateur, AWS SSO redirige la demande au service d'authentification AWS SSO en tenant compte de l'annuaire associé à son adresse e-mail. Une fois authentifiés, les utilisateurs disposent d'un accès SSO à tous les comptes AWS et les applications logicielles tierces en tant que service (SaaS) qui s'affichent dans le portail sans invites de connexion supplémentaires. Cela signifie que les utilisateurs n'ont plus besoin d'assurer le suivi de plusieurs identifiants de compte pour les différentes applications AWS attribuées qu'ils utilisent quotidiennement.

Jeux d'autorisations

Un jeu d'autorisations est un ensemble de stratégies définies par l'administrateur qu'AWS SSO utilise pour déterminer les autorisations effectives d'accès à un compte AWS. Les jeux d'autorisations peuvent contenir des stratégies gérées par AWS ou des stratégies personnalisées stockées dans AWS SSO. Les stratégies sont essentiellement des documents qui servent de conteneurs pour une ou plusieurs instructions d'autorisation. Ces déclarations représentent des contrôles d'accès (accorder ou refuser) qui déterminent les tâches que les utilisateurs peuvent ou ne peuvent pas effectuer dans le compte AWS.

Les jeux d'autorisations sont stockés dans AWS SSO et ne sont utilisés que pour les comptes AWS. Ils ne sont pas utilisés pour gérer l'accès aux applications cloud. Les jeux d'autorisations sont en fin de compte

créés sous forme de rôles IAM dans un compte AWS, avec des stratégies d'approbation qui permettent aux utilisateurs d'assumer le rôle via AWS SSO.

Gérer votre annuaire

Vous pouvez configurer votre annuaire dans AWS SSO pour déterminer où vos utilisateurs et groupes sont stockés. Une fois l'annuaire configuré, vous pouvez rechercher des utilisateurs ou des groupes dans votre annuaire pour leur accorder un accès à authentification unique à des comptes AWS, à des applications cloud, ou aux deux.

AWS SSO vous fournit automatiquement un annuaire par défaut, que vous pouvez utiliser pour gérer vos utilisateurs et groupes dans AWS SSO. Si vous choisissez de les stocker dans AWS SSO, créez vos utilisateurs et vos groupes et attribuez leur niveau d'accès à vos comptes et applications AWS. Vous pouvez également choisir de Connexion de AWS SSO à un annuaire Active Directory sur site (p. 12) ou Connexion de AWS SSO à un annuaire AWS Managed Microsoft AD (p. 12) avec AWS Directory Service.

> **Note**
>
> AWS SSO ne prend en charge aucun Simple AD SAMBA4 comme annuaire connecté.

Rubriques

Gérer votre annuaire AWS SSO

AWS Single Sign-On vous fournit un annuaire par défaut dans lequel vous pouvez stocker vos utilisateurs et vos groupes. Si vous choisissez de les stocker dans AWS SSO, il vous suffit d'effectuer les opérations suivantes :

1. Créer vos utilisateurs et groupes.
2. Ajouter vos utilisateurs en tant que membres aux groupes.
3. Attribuer aux groupes avec le niveau d'accès souhaité à vos comptes et applications AWS.

> **Note**
>
> Les utilisateurs et les groupes que vous créez dans votre annuaire AWS SSO sont disponibles dans AWS SSO uniquement.

Si vous préférez gérer les utilisateurs dans AWS Managed Microsoft AD, vous pouvez cesser d'utiliser votre annuaire AWS SSO à tout moment et connecter AWS SSO à votre annuaire Microsoft AD avec AWS Directory Service. Pour plus d'informations, consultez Connexion à votre annuaire Microsoft AD (p. 11).

Rubriques

Ajouter des utilisateurs

Utilisez la procédure suivante pour ajouter des utilisateurs à votre annuaire AWS SSO

Pour ajouter un utilisateur

1. Ouvrez la console AWS SSO .
2. Dans Dashboard (Tableau de bord), choisissez Manage your directory (Gérer votre annuaire).
3. Sur la page Directory (Annuaire), choisissez l'onglet Users (Utilisateurs), puis Add user (Ajouter un utilisateur).
4. Sur la page Add user (Ajouter un utilisateur), indiquez les informations requises suivantes :
   a. Adresse e-mail
   b. Password (Mot de passe) – Choisissez parmi les options suivantes pour envoyer le mot de passe de l'utilisateur.
      i. Send an email to the user with password setup instructions (Envoyer un e-mail à l'utilisateur avec les instructions de configuration du mot de passe) – Cette option envoie automatiquement à l'utilisateur un e-mail depuis Amazon Web Services et invite l'utilisateur au nom de votre entreprise à accéder au portail utilisateur AWS SSO.
      ii. Generate a one-time password that you can share with the user (Générer un mot de passe à usage unique que vous pouvez partager avec l'utilisateur) – Cette option vous fournit les détails d'URL de portail utilisateur et de mot de passe que vous pouvez envoyer manuellement à l'utilisateur à partir de votre adresse e-mail.
   c. Prénom
   d. Nom
   e. Nom d'affichage

      Note

      (Facultatif) Vous pouvez fournir des attributs supplémentaires comme Employee ID (ID employé) et Office 365 Immutable ID (ID Office 365 inchangeable) pour aider à mapper l'identité de l'utilisateur dans AWS SSO avec certaines applications métier que l'utilisateur a besoin d'utiliser.
5. Choisissez Next: Groups (Suivant : Groupes).
6. Sélectionnez un ou plusieurs groupes auquel l'utilisateur doit appartenir, puis choisissez Add user (Ajouter un utilisateur).

Ajouter des groupes

Utilisez la procédure suivante pour ajouter des groupes à votre annuaire AWS SSO

Pour ajouter un groupe

1. Ouvrez la console AWS SSO .
2. Dans Dashboard (Tableau de bord), choisissez Manage your directory (Gérer votre annuaire).
3. Sur la page Directory (Annuaire), choisissez l'onglet Groups (Groupes), puis Create group (Créer un groupe).
4. Dans la boîte de dialogue Create group (Créer un groupe), saisissez un Group name (Nom de groupe) et une Description. La description doit fournir des détails sur les autorisations qui ont été (ou seront) attribuées au groupe.
5. Sélectionnez Create (Créer).

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 annuaire AWS SSO.

Pour ajouter un utilisateur en tant que membre d'un groupe

1. Ouvrez la console AWS SSO .
2. Dans Dashboard (Tableau de bord), choisissez Manage your directory (Gérer votre annuaire).
3. Sur la page Directory (Annuaire), choisissez l'onglet Groups (Groupes), puis choisissez un groupe dans la liste.
4. Sur la page Details (Détails) du groupe, sous Group members (Membres du groupe), choisissez Add users (Ajouter des utilisateurs).
5. Sur la page Add users to group (Ajouter des utilisateurs au groupe), recherchez les utilisateurs que vous souhaitez ajouter en tant que membres. Activez ensuite la case à cocher en regard de chacun d'entre eux.
6. Choisissez Add user.

Modifier les propriétés d'un utilisateur

Utilisez la procédure suivante pour modifier les propriétés d'un utilisateur dans votre annuaire AWS SSO.

Pour modifier des les propriétés d'un utilisateur

1. Ouvrez la console AWS SSO .
2. Dans Dashboard (Tableau de bord), choisissez Manage your directory (Gérer votre annuaire).
3. Sur la page Directory (Annuaire), choisissez l'onglet Users (Utilisateurs), puis sélectionnez l'utilisateur à modifier.
4. Sur la page Details (Détails) de l'utilisateur, choisissez Edit user (Modifier l'utilisateur).
5. Sur la page Edit user details (Modifier les détails de l'utilisateur), mettez à jour les propriétés selon vos besoins, puis choisissez Save changes (Enregistrer les modifications).

   Note

   (Facultatif) Vous pouvez modifier des attributs supplémentaires comme Employee ID (ID employé) et Office 365 Immutable ID (ID Office 365 inchangeable) pour aider à mapper l'identité de l'utilisateur dans AWS SSO avec certaines applications métier que les utilisateurs ont besoin d'utiliser.

Désactiver un utilisateur

Lorsque vous désactivez un utilisateur, vous ne pouvez pas modifier ses détails, réinitialiser son mot de passe, l'ajouter à un groupe ou afficher son appartenance à un groupe. Utilisez la procédure suivante pour désactiver un utilisateur dans votre annuaire AWS SSO

Pour désactiver un utilisateur

1. Ouvrez la console AWS SSO .
2. Dans Dashboard (Tableau de bord), choisissez Manage your directory (Gérer votre annuaire).
3. Sur la page Directory (Annuaire), choisissez l'onglet Users (Utilisateurs), puis sélectionnez l'utilisateur à désactiver.

4. Dans la boîte de dialogue Disable user (Désactiver un utilisateur), choisissez Disable user (Désactiver un utilisateur).

   Note

   La désactivation d'un utilisateur empêche celui-ci de pouvoir se connecter au portail utilisateur.

Réinitialiser un mot de passe utilisateur

Utilisez la procédure suivante pour réinitialiser le mot de passe d'un utilisateur dans votre annuaire AWS SSO.

Pour réinitialiser un mot de passe utilisateur

1. Ouvrez la console AWS SSO .
2. Dans Dashboard (Tableau de bord), choisissez Manage your directory (Gérer votre annuaire).
3. Sur la page Directory (Annuaire), choisissez l'onglet Users (Utilisateurs), puis sélectionnez l'utilisateur dont vous voulez réinitialiser le mot de passe.
4. Dans la boîte de dialogue Reset password (Réinitialiser le mot de passe), sélectionnez l'une des options suivantes, puis choisissez Reset password (Réinitialiser le mot de passe) :

   a. Send an email to the user with instructions to reset the password (Envoyer un e-mail à l'utilisateur avec des instructions pour réinitialiser le mot de passe) – Cette option envoie automatiquement à l'utilisateur un e-mail depuis Amazon Web Services avec une procédure pour réinitialiser son passe.

   b. Generate a one-time password and share the password with the user (Générer un mot de passe à usage unique et le partager avec l'utilisateur) – Cette option vous fournit les détails d'URL de portail utilisateur et de mot de passe que vous pouvez envoyer manuellement à l'utilisateur à partir de votre adresse e-mail.

Connexion à votre annuaire Microsoft AD

AWS Single Sign-On permet aux administrateurs de connecter leur annuaire AWS Managed Microsoft AD ou Active Directory (AD) sur site à l'aide d'AWS Directory Service. L'annuaire Microsoft AD définit le groupe d'identités que les administrateurs peuvent extraire lorsqu'ils utilisent la console AWS SSO pour attribuer un accès par authentification unique (SSO). Après avoir connecté leur annuaire d'entreprise à AWS SSO, les administrateurs peuvent ensuite accorder à leurs utilisateurs ou groupes Active Directory l'accès à des comptes et/ou des applications cloud AWS.

AWS Directory Service vous aide à configurer et exécuter un annuaire AWS Managed Microsoft AD autonome hébergé dans le cloud AWS. Vous pouvez également utiliser AWS Directory Service pour connecter vos ressources AWS à un annuaire Microsoft Active Directory sur site existant. Pour configurer AWS Directory Service pour qu'il fonctionne avec votre annuaire Active Directory sur site, vous devez commencer par configurer les relations d'approbation en vue d'étendre l'authentification du site au cloud.

Note

AWS SSO ne prend en charge aucun Simple AD SAMBA4 comme annuaire connecté.

Rubriques

Connexion de AWS SSO à un annuaire AWS Managed Microsoft AD

Utilisez la procédure suivante pour connecter un annuaire AWS Managed Microsoft AD géré par AWS Directory Service à AWS SSO.

Pour connecter AWS SSO à AWS Managed Microsoft AD

1. Ouvrez la console AWS SSO .

   Note

   Vérifiez que la console AWS SSO utilise l'une des régions dans lesquelles se trouve votre annuaire AWS Managed Microsoft AD avant de passer à l'étape suivante.
2. Dans Dashboard (Tableau de bord), choisissez Manage your directory (Gérer votre annuaire).
3. Sur la page Directory (Annuaire), procédez de la façon suivante :

   a. Sous Available directories (Annuaires disponibles), sélectionnez l'annuaire AWS Managed Microsoft AD auquel vous voulez qu'AWS SSO se connecte.

   b. Sous User portal URL (URL du portail utilisateur), saisissez le préfixe à utiliser pour l'URL de connexion au portail utilisateur.
4. Choisissez Connect directory (Connecter l'annuaire).

Connexion de AWS SSO à un annuaire Active Directory sur site

Les utilisateurs de votre annuaire Active Directory sur site peut également avoir un accès SSO à des comptes et applications cloud AWS dans le portail utilisateur AWS SSO. Pour ce faire, AWS Directory Service offre les deux options suivantes :

- Créer une relation d'approbation bidirectionnelle – Les relations d'approbation bidirectionnelle créées entre AWS Managed Microsoft AD et un annuaire Active Directory sur site permettent aux utilisateurs sur site de se connecter à l'aide de leurs informations d'identification d'entreprise à divers services et applications métier AWS. Les relations d'approbation unidirectionnelles ne fonctionnent pas avec AWS SSO. Pour plus d'informations sur la configuration d'une relation d'approbation bidirectionnelle, consultez Quand créer une relation d'approbation dans le AWS Directory Service Administration Guide.
- Créer un AD Connector – AD Connector est une passerelle d'annuaire qui peut rediriger des demandes d'annuaire vers votre annuaire Active Directory sur site sans mettre d'informations en cache dans le cloud. Pour plus d'informations, consultez Connexion à un annuaire dans le AWS Directory Service Administration Guide.

  Note

  AWS SSO ne fonctionne pas avec les annuaires Simple AD SAMBA4.

Mappages d'attributs

Les mappages d'attributs sont utilisés pour mapper les types d'attribut qui existent dans AWS SSO à des attributs similaires dans un annuaire AWS Managed Microsoft AD. AWS SSO récupère les attributs

utilisateur de votre annuaire Microsoft AD et les mappe aux attributs utilisateur AWS SSO. Ces mappages d'attributs utilisateur AWS SSO sont également utilisés pour générer des assertions SAML pour vos applications cloud. Chaque application cloud détermine la liste des attributs SAML dont elle a besoin pour réussir l'authentification unique.

AWS SSO pré-remplit un ensemble d'attributs à votre place sous l'onglet Attribute mappings (Mappages d'attributs), situé dans la page de configuration de votre application. AWS SSO utilise ces attributs utilisateur pour renseigner les assertions SAML (sous forme d'attributs SAML) qui sont envoyées à l'application cloud. Ces attributs utilisateur sont ensuite extraits de votre annuaire Microsoft AD. Pour plus d'informations, consultez Mappage des attributs de votre application aux attributs AWS SSO (p. 28).

AWS SSO gère également un ensemble d'attributs à votre place dans la section Attribute mappings (Mappages d'attributs) de la page de configuration de votre annuaire. Pour plus d'informations, consultez Mappage des attributs dans AWS SSO aux attributs dans votre annuaire AWS Managed Microsoft AD (p. 15).

Attributs d'annuaire pris en charge

Le tableau suivant contient la liste complète des attributs d'annuaire AWS Managed Microsoft AD pris en charge qui peuvent être mappés aux attributs utilisateur dans AWS SSO.

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 toute combinaison d'attributs d'annuaire Microsoft AD pris en charge à mapper à un seul attribut dans AWS SSO. Par exemple, vous pouvez choisir l'attribut `preferredUsername` dans la colonne User attribute in AWS AWS SSO (Attribut utilisateur dans AWS SSO), puis le mapper à `${dir:displayname}` ou `${dir:lastname}${dir:firstname }`, ou à un seul attribut pris en charge, ou encore à toute combinaison arbitraire d'attributs pris en charge.

Attributs AWS SSO pris en charge

Le tableau suivant contient la liste complète des attributs AWS SSO pris en charge et qui peuvent être mappés aux attributs utilisateur dans votre annuaire AWS Managed Microsoft AD. Par la suite, lorsque vous aurez configuré vos mappages d'attributs d'application, vous pourrez utiliser ces mêmes attributs AWS SSO et les mapper aux attributs réels utilisés par cette application.

Attributs pris en charge dans AWS SSO
`${user:AD_GUID}`
`${user:email}`
`${user:familyName}`
`${user:firstName}`
`${user:middleName}`
`${user:name}`
`${user:preferredUsername}`
`${user:subject}`

Mappages par défaut

Le tableau suivant montre les mappages par défaut des attributs utilisateur dans AWS SSO aux attributs utilisateur dans votre annuaire AWS Managed Microsoft AD. À l'heure actuelle, AWS SSO prend uniquement en charge la liste d'attributs présentée dans la colonne User attribute in AWS SSO (Attribut utilisateur dans AWS SSO).

Attribut utilisateur dans AWS SSO	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}`

Vous pouvez modifier les mappages par défaut ou ajouter d'autres attributs à l'assertion SAML en fonction de vos besoins. Par exemple, supposons que votre application cloud nécessite l'adresse e-mail des utilisateurs dans l'attribut SAML `User.Email` et que les e-mails sont stockés dans l'attribut `windowsUpn` dans votre annuaire Microsoft AD. Pour obtenir ce mappage, vous devez effectuer des modifications dans les deux emplacements suivants de la console AWS SSO :

1. Sur la page Directory (Annuaire), sous la section Attribute mappings (Mappages d'attributs), vous devez mapper l'attribut utilisateur **`email`** à l'attribut **`${dir:windowsUpn}`** (dans la colonne Maps to this attribute in your directory (Mappé à cet attribut dans votre annuaire)).
2. Sur la page Applications, choisissez l'application dans le tableau, sélectionnez l'onglet Attribute mappings (Mappages d'attributs), puis mappez l'attribut `User.Email` à l'attribut **`${user:email}`** (dans la colonne Maps to this string value or user attribute in AWS SSO (Mappé à cette valeur de chaîne ou cet attribut utilisateur dans AWS SSO)).

Vous devez fournir chaque attribut d'annuaire dans le formulaire ${dir:**`AttributeName`**}. Par exemple, l'attribut `firstname` dans votre annuaire Microsoft AD devient `${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.

Mappage des attributs dans AWS SSO aux attributs dans votre annuaire AWS Managed Microsoft AD

Vous pouvez utiliser la procédure suivante pour spécifier la façon dont vos attributs utilisateur dans AWS SSO doivent être mappés avec les attributs correspondants dans votre annuaire Microsoft AD.

Pour mapper des attributs dans AWS SSO aux attributs dans votre annuaire

1. Ouvrez la console AWS SSO .
2. Choisissez Connected directory (Annuaire connecté).
3. Sous Attribute mappings (Mappages d'attributs), choisissez Edit attribute mappings (Modifier les mappages d'attributs).
4. Sur la page Edit attribute mappings (Modifier les mappages d'attributs), recherchez l'attribut dans AWS SSO que vous souhaitez mapper, puis saisissez une valeur dans la zone de texte. Par exemple, vous pouvez mapper l'attribut utilisateur AWS SSO **`email`** à l'attribut **`${dir:windowsUpn}`** dans l'annuaire Microsoft AD.
5. Sélectionnez Save Changes.

Modification de votre type d'annuaire

Vous pouvez modifier l'emplacement où vous stockez des utilisateurs à tout moment. Utilisez la procédure suivante pour passer d'un annuaire fourni par AWS SSO (valeur par défaut) à un annuaire AWS Managed Microsoft AD ou vice versa.

Pour modifier votre type d'annuaire

1. Ouvrez la console AWS SSO .
2. Dans Dashboard (Tableau de bord), choisissez Manage your directory (Gérer votre annuaire).
3. Sur la page Directory (Annuaire), sélectionnez Change directory (Changer d'annuaire).
4. Sur la page Change directory (Changer d'annuaire), choisissez l'annuaire vers lequel vous voulez basculer, puis Next (Suivant). Si vous passez à un annuaire Microsoft AD, vous devez choisir l'annuaire disponible dans le menu fourni.

   > **Important**
   >
   > La modification d'un annuaire supprime toutes les affectations d'utilisateur qui ont été effectuées précédemment. Vous devez manuellement les réappliquer une fois que vous avez modifié votre annuaire.
5. Choisissez Next: Review (Suivant : Vérification).
6. Une fois que vous avez lu l'avertissement et vous êtes prêt à continuer, tapez CONFIRM.
7. Choisissez Finish.

Gestion de l'accès SSO à vos comptes AWS

AWS Single Sign-On est intégré à AWS Organizations afin de permettre aux administrateurs de choisir plusieurs comptes AWS dont les utilisateurs ont besoin d'un accès par authentification unique (SSO) à AWS Management Console. Ces comptes AWS peuvent être un compte principal dans AWS Organizations ou un compte membre. Un compte principal est le compte AWS utilisé pour créer l'organisation. Le reste des comptes qui appartiennent à une organisation sont appelés comptes membres. Pour plus d'informations sur les différents types de comptes, consultez Terminologie et concepts d'AWS Organizations dans le Manuel de l'utilisateur AWS Organizations.

Une fois que vous avez attribué un accès à partir de la console AWS SSO, vous pouvez utiliser les jeux d'autorisations pour affiner davantage ce que les utilisateurs peuvent faire dans AWS Management Console. Pour plus d'informations sur les jeux d'autorisations, consultez Jeux d'autorisations (p. 19).

Les utilisateurs suivent un processus de connexion simple :

1. Les utilisateurs utilisent leurs informations d'identification d'annuaire pour se connecter au portail utilisateur.
2. Ils choisissent ensuite le nom du compte AWS qui leur donne un accès fédéré à AWS Management Console pour ce compte.
3. Les utilisateurs qui bénéficient de plusieurs jeux d'autorisations choisissent le rôle IAM à utiliser.

Les jeux d'autorisations constituent le moyen de définir des autorisations de manière centralisée dans AWS SSO pour pouvoir les appliquer à tous vos comptes AWS. Ces jeux d'autorisations sont alloués à chaque compte AWS sous la forme d'un rôle IAM. Dans le portail utilisateur, les utilisateurs peuvent extraire les informations d'identification temporaires correspondant au rôle IAM d'un compte AWS spécifique et les utiliser pour accéder à court terme à l'interface de ligne de commande AWS. Pour plus d'informations, consultez Comment obtenir les informations d'identification d'un rôle IAM pour les utiliser avec l'accès par interface de ligne de commande à un compte AWS (p. 45).

Pour utiliser AWS SSO avec AWS Organizations, vous devez commencer par Activer AWS SSO (p. 3), ce qui permet à AWS SSO de créer des Rôles liés à un service (p. 21) dans chaque compte de votre organisation AWS. Ces rôles sont créés lorsque vous avez terminé de Attribution d'un accès utilisateur (p. 17) pour un compte donné.

Vous pouvez également connecter un compte AWS qui ne fait pas partie de votre organisation en le configurant en tant qu'application SAML personnalisée dans AWS SSO. Dans ce scénario, vous allez allouer et gérer les rôles et relations d'approbation IAM qui sont requis pour activer un accès SSO. Pour en savoir plus à ce sujet, consultez Ajout et configuration d'une application SAML 2.0 personnalisée (p. 25).

Rubriques

Accès par authentification unique (SSO)

Vous pouvez attribuer à des utilisateurs dans votre annuaire connecté des autorisations sur les comptes AWS principal ou membres de votre organisation AWS Organizations en fonction de 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 à Amazon RDS dans les comptes de développement mais limiter leurs autorisations dans les comptes de production. AWS SSO configure automatiquement toutes les autorisations utilisateur nécessaires dans vos comptes AWS.

Note

Seul l'utilisateur racine du compte IAM ou un utilisateur auquel la stratégie IAM AWSSSOMasterAccountAdministrator est attachée peut accorder à des utilisateurs dans votre annuaire connecté des autorisations sur le compte AWS principal. Pour plus d'informations sur comment déléguer ces autorisations, consultez Déléguer qui peut attribuer l'accès SSO à des utilisateurs dans le compte principal (p. 18).

Attribution d'un accès utilisateur

Utilisez la procédure suivante pour attribuer un accès SSO à des utilisateurs et des groupes dans votre annuaire connecté et utiliser des jeux d'autorisations pour déterminer leur niveau d'accès.

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 des utilisateurs ou des groupes

1. Ouvrez la console AWS SSO .

   Note

   Assurez-vous que la console AWS SSO utilise la région USA Est (Virginie du Nord) (us-east-1) dans laquelle se trouve votre annuaire AWS Managed Microsoft AD avant de passer à l'étape suivante.
2. Choisissez AWS accounts (Comptes AWS).
3. Sous l'onglet AWS organization (Organisation AWS), dans la liste des comptes AWS, choisissez un compte auquel vous souhaitez attribuer l'accès.
4. Sur la page des détails de compte AWS, choisissez Assign users (Affecter des utilisateurs).
5. Dans la page Select users or groups (Sélectionner des utilisateurs ou des groupes), saisissez un nom d'utilisateur ou de groupe et choisissez Search connected directory (Rechercher dans l'annuaire connecté). Une fois que vous avez sélectionné tous les comptes auxquels vous souhaitez attribuer l'accès, choisissez Next: Permission sets (Suivant : Jeux d'autorisations). Vous pouvez spécifier plusieurs utilisateurs ou groupes en sélectionnant les comptes applicables tels qu'ils apparaissent dans les résultats de recherche.
6. Dans la page Select permission sets (Sélectionner des jeux d'autorisations), sélectionnez dans le tableau les jeux d'autorisations que vous souhaitez appliquer à l'utilisateur ou au groupe. Choisissez ensuite Finish (Terminer). Vous pouvez éventuellement choisir Create a new permission set (Créer un jeu d'autorisations) si aucune des autorisations indiquées dans le tableau ne répond à vos besoins. Pour obtenir des instructions complètes, consultez Création d'un jeu d'autorisations (p. 19).
7. Choisissez Finish (Terminer) pour lancer le processus de configuration de votre compte AWS.

   Note

   Si vous avez attribué un accès SSO à ce compte AWS pour la première fois, cette procédure crée un rôle lié à un service dans le compte. Pour plus d'informations, consultez Utilisation des rôles liés à un service pour AWS SSO (p. 39).

Important

Le processus d'affectation d'utilisateur peut prendre quelques minutes. Il importe de laisser cette page ouverte jusqu'à ce que le processus aboutisse.

Suppression d'un accès utilisateur

Utilisez cette procédure pour supprimer un accès par authentification unique (SSO) à un compte AWS pour un utilisateur ou un groupe spécifique présent dans votre annuaire connecté.

Pour supprimer un accès utilisateur à un compte AWS

1. Ouvrez la console AWS SSO .
2. Choisissez AWS accounts (Comptes AWS).
3. Dans le tableau, sélectionnez le compte AWS contenant l'utilisateur ou le groupe dont vous souhaitez supprimer l'accès.
4. Dans la page Details (Détails) du compte AWS, sous Assigned users and groups (Utilisateurs et groupes attribués), recherchez l'utilisateur ou le groupe dans le tableau. Choisissez ensuite Remove access (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).

Déléguer qui peut attribuer l'accès SSO à des utilisateurs dans le compte principal

L'attribution d'un accès à authentification unique au compte principal à l'aide de la console AWS SSO est une action avec privilèges d'accès. Par défaut, seul l'utilisateur racine d'un compte AWS ou un utilisateur auquel la stratégie gérée AWS AWSSSOMasterAccountAdministrator est attachée peut attribuer l'accès SSO au compte principal. La stratégie AWSSSOMasterAccountAdministrator assure la gestion de l'accès SSO au compte principal au sein d'une organisation AWS Organizations.

Utilisez les étapes suivantes pour déléguer des autorisations de gestion de l'accès SSO à des utilisateurs dans votre annuaire.

Pour accorder des autorisations de gestion de l'accès SSO à des utilisateurs dans votre annuaire

1. Connectez-vous à la console AWS SSO en tant qu'utilisateur racine du compte principal ou avec un autre utilisateur IAM disposant d'autorisations d'administrateur IAM sur le compte principal.
2. Utilisez la procédure Création d'un jeu d'autorisations (p. 19) pour créer un jeu d'autorisations. Lorsque vous accédez à l'étape 5c, sélectionnez l'option Attach AWS managed policies (Attacher des stratégies gérées AWS). Dans la liste des stratégies IAM qui apparaît dans le tableau, choisissez la stratégie gérée AWS AWSSSOMasterAccountAdministrator. Cette stratégie accorde des autorisations à tout utilisateur qui reçoit l'accès à ce jeu d'autorisations par la suite.
3. Utilisez la procédure Attribution d'un accès utilisateur (p. 17) pour attribuer les utilisateurs appropriés au jeu d'autorisations que vous venez de créer.
4. Communiquez les instructions suivantes à ces utilisateurs : Une fois qu'ils se sont connectés au portail utilisateur et qu'ils ont sélectionné l'icône de compte AWS, ils doivent choisir le nom de rôle IAM approprié pour être authentifié avec les autorisations que vous venez de déléguer.

Jeux d'autorisations

Les jeux d'autorisations définissent le niveau d'accès que les utilisateurs et les groupes ont au compte AWS. Les jeux d'autorisations sont stockés dans AWS SSO et alloués au compte AWS en tant que rôles IAM. Vous pouvez attribuer plus d'un jeu d'autorisations à un utilisateur. Les utilisateurs qui possèdent plusieurs jeux d'autorisations doivent en choisir un seul lorsqu'ils se connectent au portail utilisateur. (Ils voient ces jeux d'autorisations comme étant des rôles IAM). Pour plus d'informations, consultez Jeux d'autorisations (p. 6).

Création d'un jeu d'autorisations

Utilisez cette procédure pour créer un jeu d'autorisations basé sur une stratégie d'autorisations personnalisées que vous créez et/ou des stratégies gérées par AWS prédéfinies qui existent dans IAM.

Pour créer un jeu d'autorisations

1. Ouvrez la console AWS SSO .
2. Choisissez AWS accounts (Comptes AWS).
3. Sélectionnez l'onglet Permission sets (Jeux d'autorisations).
4. Choisissez Create permission set (Créer un jeu d'autorisations).
5. Dans la boîte de dialogue Create new permission set (Créer un jeu d'autorisations), choisissez l'une des options suivantes, puis suivez les instructions fournies pour cette option :

   - Utiliser une stratégie de fonction professionnelle
     1. Sous Select job function policy (Sélectionner une stratégie de fonction professionnelle), sélectionnez l'une des stratégies de fonctions professionnelles IAM par défaut dans la liste. Pour plus d'informations, consultez Stratégies gérées par AWS pour les activités professionnelles.
     2. Sélectionnez Create (Créer).
   - Créer un jeu d'autorisations personnalisé
     1. Sous Create a custom permission set (Créer un jeu d'autorisations personnalisé), saisissez un nom qui permettra d'identifier ce jeu d'autorisations dans AWS SSO. Ce nom sera visible dans le portail utilisateur comme un rôle IAM pour tous les utilisateurs qui y ont accès.
     2. (Facultatif) Vous pouvez également saisir une description. Cette description ne s'affichera que dans la console AWS SSO et ne sera pas visible par les utilisateurs du portail utilisateur.
     3. Choisissez Attach AWS managed policies (Attacher des stratégies gérées par AWS) ou Create a custom permissions policy (Créer une stratégie d'autorisations personnalisées). Ou sélectionnez les deux si vous avez besoin d'associer plusieurs types de stratégie à ce jeu d'autorisations.
     4. Si vous avez choisi Attach AWS managed policies (Attacher des stratégies gérées par AWS), sous Attach AWS managed policies (Attacher des stratégies gérées par AWS), sélectionnez dans la liste jusqu'à 10 stratégies gérées par AWS relatives à des tâches ou des services.
     5. Si vous avez choisi Create a custom permissions policy (Créer une stratégie d'autorisations personnalisées), sous Create a custom permissions policy (Créer une stratégie d'autorisations personnalisées), collez un document de stratégie contenant vos autorisations préférées. Pour obtenir la liste des exemples de stratégies à utiliser pour déléguer des tâches AWS SSO, consultez Exemples de stratégies gérées par le client (p. 35).

        Pour plus d'informations sur le langage d'access policy, consultez Présentation des stratégies dans le IAM Guide de l'utilisateur. Pour tester les conséquences de cette stratégie avant d'appliquer les modifications, utilisez le simulateur de stratégie IAM.
     6. Sélectionnez Create (Créer).

Suppression de jeux d'autorisations

Utilisez cette procédure pour supprimer un ou plusieurs jeux d'autorisations afin de les rendre inutilisables par les comptes AWS de l'organisation.

> Note
>
> Tous les utilisateurs et groupes auxquels est affecté ce jeu d'autorisations ne pourront plus se connecter, quel que soit le compte AWS qui l'utilise.

Pour supprimer un jeu d'autorisations à partir d'un compte AWS

1. Ouvrez la console AWS SSO .
2. Choisissez AWS accounts (Comptes AWS).
3. Choisissez l'onglet Permission sets (Jeux d'autorisations).
4. Sélectionnez le jeu d'autorisations que vous voulez supprimer, puis Delete (Supprimer).
5. Dans la boîte de dialogue Delete permission set (Supprimer un jeu d'autorisations), choisissez Delete (Supprimer).

Définir la durée de la session

Pour chaque autorisation définie, vous pouvez spécifier une durée de session pour contrôler la durée pendant laquelle un utilisateur peut être connecté à un compte AWS. Lorsque la durée spécifiée s'est écoulée, AWS déconnecte l'utilisateur de la session. Pour les comptes AWS, AWS SSO utilise ce paramètre pour définir la durée de session maximale du rôle IAM que vous utilisez pour générer la session d'un utilisateur. La durée de session que vous spécifiez pour un jeu d'autorisations donné s'applique à AWS Management Console et la session AWS Command Line Interface (CLI).

Lorsque vous créez un nouveau jeu d'autorisations, celui-ci est configuré avec la longueur de session par défaut d'1 heure (en secondes). La longueur de session minimale est d'1 heure et peut être configurée à 12 heures maximum.

> 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.

Une fois qu'un jeu d'autorisations a été créé, vous pouvez le mettre à jour ultérieurement pour appliquer une nouvelle durée de session. Lorsque vous réappliquez le jeu d'autorisations à vos comptes AWS, la valeur de durée de session maximale du rôle IAM est mise à jour. Utilisez la procédure suivante pour modifier la longueur de durée de session pour un jeu d'autorisations.

Pour définir la durée de session

1. Ouvrez la console AWS SSO .
2. Choisissez AWS accounts (Comptes AWS).
3. Choisissez l'onglet Permission sets (Jeux d'autorisations).
4. Choisissez le nom du jeu d'autorisations qui aura la nouvelle durée de session.
5. Sous l'onglet Permissions (Autorisations), en regard de Session duration (Durée de la session), choisissez Edit (Modifier).
6. Sur la page Edit session duration (Modifier la durée de la session), en regard de New session duration (Nouvelle durée de session), choisissez une nouvelle valeur de longueur de session, puis Continue (Continuer).
7. Sélectionnez dans la liste les comptes AWS auxquels vous souhaitez appliquer la nouvelle valeur de durée de session, puis choisissez Reapply permission set (Réappliquer le jeu d'autorisations).

Fournisseur d'identité IAM

Lorsque vous ajoutez un accès SSO à un compte AWS, AWS SSO crée un fournisseur d'identité IAM dans chaque compte AWS. Les fournisseurs d'identité IAM vous permettent de mieux sécuriser votre compte AWS, car vous n'avez pas à distribuer ou intégrer d'informations d'identification de sécurité à long terme, comme des clés d'accès IAM, dans votre application.

Réparation du fournisseur d'identité IAM

Utilisez la procédure suivante pour réparer votre fournisseur d'identité qui a été supprimé ou modifié.

Pour réparer un fournisseur d'identité pour un compte AWS

1. Ouvrez la console AWS SSO .
2. Choisissez AWS accounts (Comptes AWS).
3. Dans le tableau, sélectionnez le compte AWS qui est associé au fournisseur d'identité que vous souhaitez réparer.
4. Sur la page des détails du compte AWS, sous IAM identity provider (Fournisseur d'identité IAM), choisissez Repair identity provider (Réparer un fournisseur d'identité).

Suppression du fournisseur d'identité IAM

Utilisez la procédure suivante pour supprimer le fournisseur d'identité IAM dans AWS SSO.

Pour supprimer le fournisseur d'identité IAM dans AWS SSO

1. Ouvrez la console de gestion AWS SSO
2. Choisissez AWS accounts (Comptes AWS)
3. Dans le tableau, sélectionnez le compte AWS qui est associé au fournisseur d'identité IAM que vous souhaitez supprimer.
4. Dans la page Details (Détails) du compte AWS, sous IAM identity provider (Fournisseur d'identité IAM), choisissez Remove identity provider (Supprimer le fournisseur d'identité).

Rôles liés à un service

Les rôles liés à un service sont des autorisations IAM prédéfinies qui permettent à AWS SSO de déléguer et faire appliquer quels utilisateurs ont un accès SSO aux comptes AWS spécifiques de votre organisation AWS. Le service configure cette fonctionnalité en allouant un rôle lié à un service dans chaque compte AWS de son organisation. Il permet alors à d'autres services AWS comme AWS SSO d'utiliser ces rôles pour effectuer les tâches relatives au service. Pour plus d'informations, consultez AWS Organizations et rôles liés au service.

Pendant le processus Activer AWS SSO (p. 3) pour la première fois, le service AWS Organizations accorde à AWS SSO les autorisations requises pour créer des rôles IAM dans l'un de ses comptes AWS. À ce stade, AWS SSO ne crée pas de rôles dans les comptes AWS. Il crée un rôle lié à un service dans un compte AWS lorsque vous avez utilisé la console AWS SSO pour spécifier le compte auquel vous souhaitez attribuer un accès SSO. Pour plus d'informations, consultez Gestion de l'accès SSO à vos comptes AWS (p. 16).

Les rôles liés à un service qui sont créés dans chaque compte AWS sont nommés `AWSServiceRoleForSSO`. Pour plus d'informations, consultez Utilisation des rôles liés à un service pour AWS SSO (p. 39).

Gestion de l'accès SSO à vos applications

Avec AWS Single Sign-On, vous pouvez facilement contrôler qui doit avoir un accès par authentification unique (SSO) à vos applications cloud. Les utilisateurs bénéficient d'un accès en un clic à ces applications une fois qu'ils se sont connectés à leur portail utilisateur avec leurs informations d'identification d'annuaire.

AWS SSO communique de façon sécurisée avec ces applications via une relation d'approbation entre AWS SSO et le service de l'application. Cette relation d'approbation est créée lorsque vous ajoutez l'application à l'aide de la console AWS SSO et que vous la configurez avec les métadonnées appropriées tant pour le service AWS SSO que pour le fournisseur de services.

Une fois que l'application a été ajoutée correctement à la console AWS SSO, vous pouvez gérer les utilisateurs ou les groupes qui ont besoin d'autorisations pour l'application. Par défaut, lorsque vous ajoutez une application, aucun utilisateur n'est affecté à cette application. En d'autres termes, les applications nouvellement ajoutées à la console AWS SSO sont inaccessibles tant que vous ne leur avez pas attribué d'utilisateurs. AWS SSO prend en charge les types d'application suivants :

- Applications cloud
- Applications Security Assertion Markup Language (SAML 2.0) personnalisées

Vous pouvez également accorder à vos employés l'accès à AWS Management Console pour un compte AWS de votre organisation. Pour en savoir plus à ce sujet, consultez Gestion de l'accès SSO à vos comptes AWS (p. 16).

Les sections suivantes expliquent comment configurer l'accès utilisateur à vos logiciels tiers en tant que service (SaaS) et à toutes les applications personnalisées qui prennent en charge la fédération d'identité avec SAML 2.0.

Rubriques

Applications cloud

Vous pouvez utiliser l'assistant de configuration d'application AWS SSO pour inclure des intégrations SAML prédéfinies à de nombreuses applications cloud populaires, comme Salesforce, Box et Office 365. Pour obtenir la liste complète des applications que vous pouvez ajouter à partir de l'assistant, consultez Applications prises en charge (p. 23).

La plupart des applications cloud sont fournies avec des instructions détaillées sur la façon de configurer la relation d'approbation entre AWS SSO et le fournisseur de services de l'application. Ces instructions se trouvent sur la page de configuration des applications cloud au cours de la procédure de configuration et

une fois que l'application a été configurée. Lorsque l'application est configurée, vous pouvez en attribuer l'accès aux groupes ou utilisateurs qui en ont besoin.

Applications prises en charge

AWS SSO intègre la prise en charge des applications cloud communément utilisées suivantes.

> Note
>
> Les ingénieurs de support AWS peuvent aider les clients qui disposent de plans de support Business et Enterprise avec des tâches d'intégration qui impliquent des logiciels tiers. Pour obtenir la liste actuelle des plateformes et applications prises en charge, consultez Prise en charge de logiciels tiers sur la page des fonctions AWS Support.

Adobe Creative Cloud	Dropbox	Lucidchart	UserEcho
Aha	DruvaInSync	MangoApps	UserVoice
AnswerHub	EduBrite	NewRelic	Velpic
AppDynamics	Egnyte	Office 365	VictorOps
Assembla	eLeaP	OpsGenie	WeekDone
Atlassian	Engagedly	PagerDuty	WhosOnLocation
BambooHR	Envoy	Panopta	Workplace by Facebook
BenSelect	Evernote	ProdPad	Workstars
Bitglass	Expensify	PurelyHR	xMatters
BMCRemedyforce	EZOfficeInventory	RingCentral	Zendesk
Bonusly	Freshdesk	Salesforce	Zoho
Box	FreshService	Samanage	Zoom
BugSnag	Front	ScaleFT	
CakeHR	G Suite	ScreenSteps	
CiscoMeraki	GitHub	ServiceNow	
CiscoUmbrella	GitLab	Slack	
Citrix ShareFile	GoToMeeting	Sli.do	
Clarizen	Grovo	Smartsheet	
ClickTime	Humanity	SnapEngage	
CloudPassage	IdeaScale	SugarCRM	
Convo	Igloo	SumoLogic	
DataDog	JamaSoftware	SurveyMonkey	
Deputy	JFrog Artifactory	Syncplicity	
Deskpro	Jitbit	Tableau	

DigiCert	join.me	TalentLMS	
Dmarcian	Keeper Security	TargetProcess	
Docebo	Klipfolio	TextMagic	
DocuSign	Kudos	ThousandEyes	
Dome9	LiquidFiles	TitanFile	
Domo	LogMeInRescue	Trello	

Ajout et configuration d'une application cloud

Utilisez cette procédure pour configurer une relation d'approbation SAML entre AWS SSO et le fournisseur de services de l'application cloud. Avant de commencer cette procédure, vérifiez que vous avez le fichier d'échange de métadonnées du fournisseur de services afin de configurer plus efficacement l'approbation. Si vous n'avez pas ce fichier, vous pouvez toujours utiliser la procédure suivante pour configurer l'approbation manuellement.

Pour ajouter et configurer une application cloud

1. Dans la console AWS SSO, choisissez Applications dans le panneau de navigation de gauche, puis Add a new application (Ajouter une nouvelle application).
2. Dans la boîte de dialogue Select an application (Sélectionner une application), sélectionnez l'application que vous souhaitez ajouter depuis la liste, puis choisissez Add (Ajouter).
3. Sur la page Configure (Configurer) <nom de l'application>, sous Details (Détails), saisissez un Display name (Nom d'affichage) pour l'application. Par exemple, **`Salesforce`**.
4. Sous AWS SSO metadata (Métadonnées AWS SSO), procédez comme suit :

   a. En regard du fichier AWS SSO SAML metadata (Métadonnées SAML AWS SSO), choisissez Download (Télécharger) pour télécharger les métadonnées du fournisseur d'identité.

   b. En regard de AWS SSO certificate (Certificat AWS SSO), choisissez Download certificate (Télécharger le certificat) pour télécharger le certificat du fournisseur d'identité.

   Note

   Vous aurez besoin de ces fichiers par la suite pour configurer l'application cloud sur le site web du fournisseur de services. Suivez les instructions de ce fournisseur.
5. Sous Application properties (Propriétés de l'application), vous pouvez éventuellement spécifier des propriétés supplémentaires pour Application start URL (URL de lancement de l'application), Relay State (État du relai) et Session Duration (Durée de session). Pour plus d'informations, consultez Propriétés d'application (p. 25).
6. Sous Application metadata (Métadonnées de l'application), fournissez les valeurs pour Application ACS URL (URL ACS d'application) et Application SAML audience (Public de l'application SAML).
7. Choisissez Save changes (Enregistrer les modifications) pour enregistrer la configuration.

Applications SAML 2.0 personnalisées

Vous pouvez utiliser l'assistant de configuration d'application AWS SSO pour ajouter la prise en charge des applications qui permettent à la fédération d'identité d'utiliser SAML (Security Assertion Markup Language)

2.0. Dans la console, configurez ces applications en choisissant Custom SAML 2.0 application (Application SAML 2.0 personnalisée) dans le sélecteur d'applications. La plupart des étapes de configuration d'une application SAML personnalisée sont les mêmes que celles d'une application cloud.

Cependant, vous devez également fournir d'autres mappages d'attributs SAML personnalisés pour une application SAML personnalisée afin que AWS SSO sache comment renseigner correctement l'assertion SAML pour votre application. Vous pouvez fournir ces mappages d'attributs SAML supplémentaires lorsque vous configurez l'application pour la première fois. Vous pouvez également fournir des mappages d'attributs SAML dans la page des détails de l'application qui est accessible dans la console AWS SSO.

Ajout et configuration d'une application SAML 2.0 personnalisée

Utilisez cette procédure pour configurer une relation d'approbation SAML entre AWS SSO et le fournisseur de services de votre application personnalisée. 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 ajouter et configurer une application SAML personnalisée

1. Dans la console AWS SSO, choisissez Applications dans le panneau de navigation de gauche. Choisissez ensuite Add a new application (Ajouter une nouvelle application).
2. Dans la boîte de dialogue Select an application (Sélectionner une application), sélectionnez Custom SAML 2.0 application (Application SAML 2.0 personnalisée) dans la liste, puis choisissez Configure application (Configurer l'application).
3. Sur la page Configure (Configurer) **<**nom de l'application personnalisée**>**, sous Details (Détails), saisissez un Display name (Nom d'affichage) pour l'application. Par exemple, **`MyApp`**.
4. Sous AWS SSO metadata (Métadonnées AWS SSO), procédez comme suit :

   a. En regard du fichier AWS SSO SAML metadata (Métadonnées SSO SAML), cliquez sur Download (Télécharger) pour télécharger les métadonnées du fournisseur d'identité.

   b. En regard de AWS SSO certificate (Certificat AWS SSO), cliquez sur Download certificate (Télécharger le certificat) 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.
5. Sous Application properties (Propriétés de l'application), vous pouvez éventuellement spécifier des propriétés supplémentaires pour Application start URL (URL de lancement de l'application), Relay State (État du relai) et Session Duration (Durée de session). Pour plus d'informations, consultez Propriétés d'application (p. 25).
6. Sous Application metadata (Métadonnées de l'application), fournissez les valeurs pour Application ACS URL (URL ACS d'application) et Application SAML audience (Public de l'application SAML).
7. Choisissez Save changes (Enregistrer les modifications) pour enregistrer la configuration.

Propriétés d'application

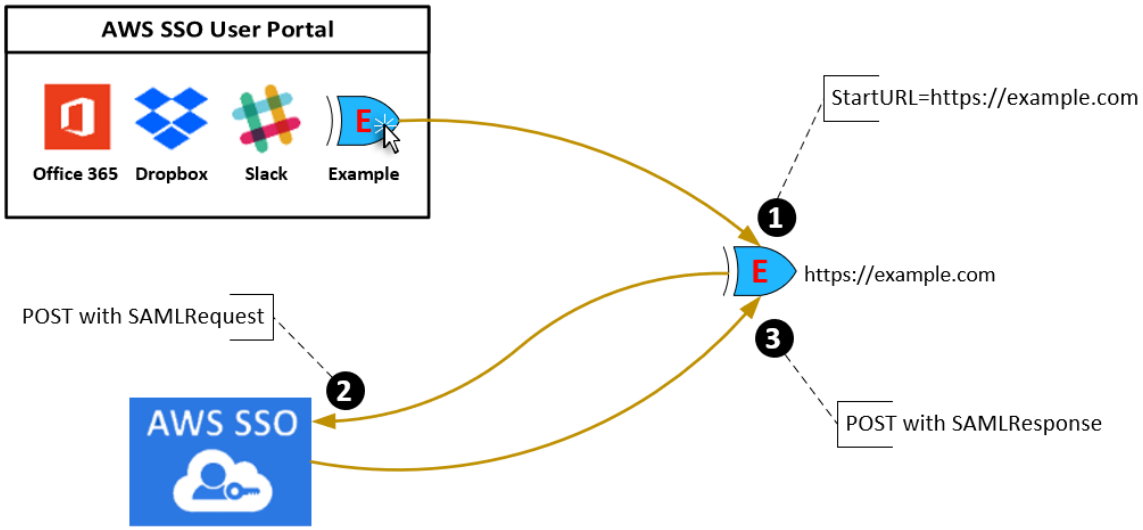
Dans, AWS SSO vous pouvez personnaliser l'expérience utilisateur en configurant les propriétés d'applications supplémentaires suivantes.

URL de lancement de l'application

Vous utilisez une URL de lancement d'application pour démarrer le processus de fédération avec votre application. Cette propriété est généralement utilisée pour une application qui prend uniquement en charge les liaisons initiées par le fournisseur de services.

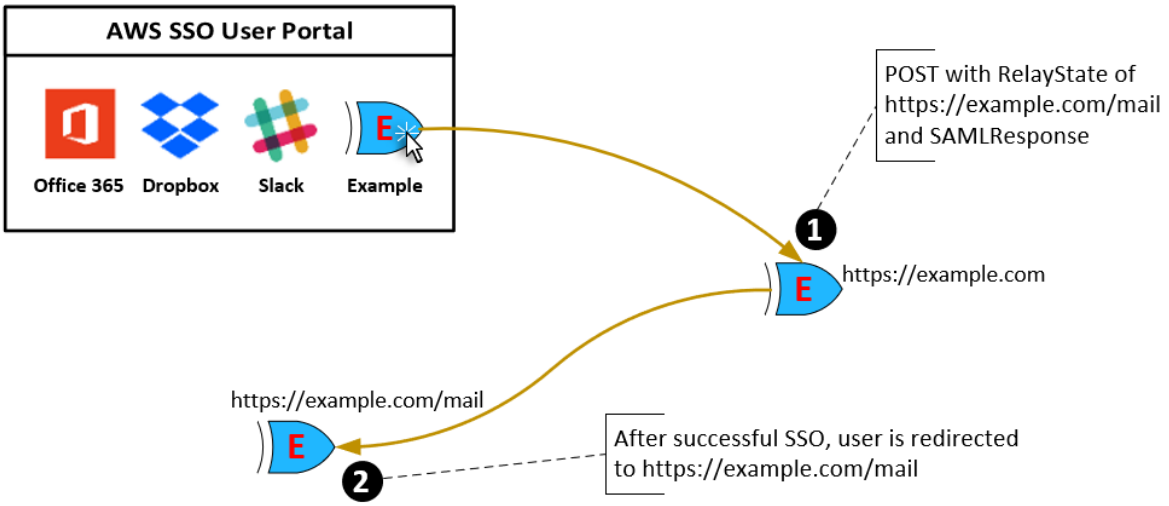
Les étapes et le schéma suivants illustrent le flux de travail d'authentification de l'URL de lancement d'application lorsqu'un utilisateur choisit une application dans le portail utilisateur :

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` avec une demande `SAMLRequest` à AWS SSO.
3. AWS SSO renvoie ensuite un `HTML POST` avec une réponse `SAMLResponse` à l'application.



État de 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 celle-ci configurée, AWS SSO envoie la valeur d'état de relais avec une réponse SAML à l'application.



Durée de la session

La durée de la session est la durée pendant laquelle les sessions utilisateur de l'application sont valides. Pour SAML 2.0, ce paramètre est utilisé pour définir la date `NotOnOrAfter` des éléments de l'assertion SAML : `saml2:SubjectConfirmationData` et `saml2:Conditions`.

La durée de la session peut être interprétée par les applications des façons suivantes :

- Les applications peuvent utiliser cette durée pour déterminer combien de temps l'assertion SAML est valide et ne la prennent pas compte pour choisir la durée autorisée pour l'utilisateur.
- Les applications peuvent l'utiliser pour déterminer la durée maximale autorisée pour la session de l'utilisateur et peuvent générer une session utilisateur avec 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.

Attribution d'un accès utilisateur

Utilisez la procédure suivante pour attribuer aux utilisateurs un accès SSO aux applications cloud ou aux applications SAML 2.0 personnalisées.

> **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 des utilisateurs ou des groupes

1. Ouvrez la console AWS SSO .

   > **Note**
   >
   > Assurez-vous que la console AWS SSO utilise la région USA Est (Virginie du Nord) dans laquelle se trouve votre annuaire AWS Managed Microsoft AD avant de passer à l'étape suivante.

2. Choisissez Applications.
3. Dans la liste des applications, choisissez une application à laquelle vous souhaitez attribuer l'accès.
4. Sur la page des détails de l'application, sélectionnez l'onglet Assigned users (Utilisateurs affectés). Choisissez ensuite Assign users (Affecter des utilisateurs).
5. Dans la boîte de dialogue Assign users (Affecter des utilisateurs), saisissez un nom d'utilisateur ou de groupe. Choisissez ensuite Search connected directory (Rechercher dans l'annuaire connecté). 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).

Suppression d'un accès utilisateur

Utilisez la procédure suivante pour supprimer un accès utilisateur à des applications cloud ou des applications SAML 2.0 personnalisées.

Pour supprimer un accès utilisateur à une application

1. Ouvrez la console AWS SSO .
2. Choisissez Applications.
3. Dans la liste des applications, choisissez une application à laquelle vous souhaitez supprimer l'accès.
4. Dans la page des détails de l'application, sélectionnez l'onglet Assigned users (Utilisateurs affectés), l'utilisateur ou le groupe que vous souhaitez supprimer, puis choisissez Remove (Supprimer).
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).

Mappage des attributs de votre application aux attributs AWS SSO

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 la façon dont les attributs utilisateur des applications doivent être mappés aux attributs correspondants dans AWS SSO.

Pour mapper les attributs d'application aux attributs dans AWS SSO

1. Ouvrez la console AWS SSO .
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 l'onglet Attribute mappings (Mappages d'attributs).
5. Choisissez Add new attribute mapping (Ajouter un nouveau mappage d'attributs).
6. Dans la première zone de texte, saisissez l'attribut de l'application.
7. Dans la deuxième zone de texte, saisissez l'attribut dans AWS SSO que vous souhaitez mapper à l'attribut d'application. Par exemple, vous pouvez mapper l'attribut d'application **`Username`** à l'attribut utilisateur AWS SSO **`email`**. Pour afficher la liste des attributs utilisateur autorisés dans AWS SSO, consultez le tableau dans Mappages d'attributs (p. 12).
8. Dans la troisième colonne du tableau, sélectionnez dans le menu le format approprié de l'attribut.
9. Sélectionnez Save Changes.

Authentification et contrôle d'accès pour AWS SSO

L'accès à AWS SSO requiert des informations d'identification qu'AWS peut utiliser pour authentifier vos demandes. Ces informations d'identification doivent disposer d'autorisations pour accéder aux ressources AWS comme une application AWS SSO.

L'authentification au portail utilisateur AWS SSO est contrôlée par l'annuaire que vous avez connecté à AWS SSO. Toutefois, l'autorisation pour les comptes AWS disponibles aux utilisateurs finaux depuis le portail utilisateur est déterminée par deux facteurs :

1. À qui a été attribué l'accès à ces comptes AWS dans la console AWS SSO. Pour plus d'informations, consultez Accès par authentification unique (SSO) (p. 16).
2. Le niveau d'autorisations accordé aux utilisateurs finaux dans la console AWS SSO pour leur autoriser un accès approprié à ces comptes AWS. Pour plus d'informations, consultez Jeux d'autorisations (p. 19).

Les sections suivantes expliquent comment vous, en tant qu'administrateur, pouvez contrôler l'accès à la console AWS SSO ou pouvez déléguer, à partir de la console AWS SSO, un accès administratif pour les tâches quotidiennes.

Authentification

Vous pouvez utiliser les types d'identité suivants pour accéder à AWS :

- Utilisateur racine d'un compte AWS – Lorsque vous créez un compte AWS, vous commencez avec une seule identité de connexion disposant d'un accès complet à tous les services et ressources AWS du compte. Cette identité est appelée la utilisateur racinedu compte AWS et elle est accessible après connexion à l'aide de l'adresse e-mail et du mot de passe utilisés pour la création du compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes, y compris pour les tâches administratives. Au lieu de cela, respectez la bonne pratique qui consiste à avoir recours à l'utilisateur racine uniquement pour créer le premier utilisateurIAM. Ensuite, mettez en sécurité les informations d'identification de l'utilisateur racine et utilisez-les pour effectuer uniquement certaines tâches de gestion des comptes et des services.
- Utilisateur IAM– Un utilisateur IAM est une identité au sein de votre compte AWS qui dispose d'autorisations personnalisées spécifiques (par exemple, des autorisations pour créer a directory dans AWS SSO). Vous pouvez utiliser un nom d'utilisateur et un mot de passe IAM pour vous connecter aux pages web AWS sécurisées telles que AWS Management Console, les forums de discussion AWS et le AWS Support Center.

  En plus d'un nom d'utilisateur et d'un mot de passe, vous pouvez générer des clés d'accès pour chaque utilisateur. Vous pouvez utiliser ces clés lorsque vous accédez aux services AWS par programmation, soit par le biais d'un kit SDK soit à l'aide d'AWS Command Line Interface (CLI). Les outils de l'interface

de ligne de commande et les kits SDK utilisent les clés d'accès pour signer de façon cryptographique votre demande. Si vous n'utilisez pas les outils AWS, vous devez signer la demande vous-même. AWS SSO supports Signature Version 4, protocole permettant l'authentification des demandes d'API entrantes. Pour plus d'informations sur l'authentification des demandes, consultez Processus de signature Signature Version 4 dans le document AWS General Reference.

- Rôle IAM – Un rôle IAM est une identité IAM que vous pouvez créer dans votre compte et qui dispose d'autorisations spécifiques. Un rôle IAM est similaire à un utilisateur IAM, car il s'agit d'une identité AWS avec des stratégies d'autorisation qui déterminent ce que l'identité peut et ne peut pas faire dans AWS. En revanche, au lieu d'être associé de manière unique à une personne, un rôle est conçu pour être assumé par tout utilisateur qui en a besoin. En outre, un rôle ne dispose pas d'informations d'identification standard à long-terme comme un mot de passe ou des clés d'accès associées. Au lieu de cela, lorsque vous adoptez un rôle, il vous fournit des informations d'identification de sécurité temporaires pour votre session de rôle. Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

  - Accès d'utilisateurs fédérés – Au lieu de créer un utilisateur IAM, vous pouvez utiliser des identités d'utilisateur préexistantes provenant d'AWS Directory Service, de l'annuaire d'utilisateurs de votre entreprise ou d'un fournisseur d'identité web. On parle alors d'utilisateurs fédérés. AWS attribue un rôle à un utilisateur fédéré lorsque l'accès est demandé via un fournisseur d'identité. Pour plus d'informations sur les utilisateurs fédérés, consultez Utilisateurs fédérés et rôles dans le IAM Guide de l'utilisateur.

  - Accès à un service AWS – Un rôle de service est un rôle IAM qu'un service assume pour effectuer des actions dans votre compte en votre nom. Lorsque vous configurez certains environnements de services AWS, vous devez définir un rôle que ce service devra assumer. Ce rôle de service doit comprendre toutes les autorisations nécessaires pour que le service puisse accéder aux ressources AWS dont il a besoin. Les rôles de service varient d'un service à un service, mais nombre d'entre eux vous permettent de choisir vos autorisations, tant que vous respectez les exigences documentées pour le service en question. Les rôles de service fournissent un accès uniquement au sein de votre compte et ne peuvent pas être utilisés pour accorder l'accès à des services dans d'autres comptes. Vous créez, modifiez et supprimez un rôle de service à partir d'IAM. Par exemple, vous pouvez créer un rôle qui permet à Amazon Redshift d'accéder à un compartiment Amazon S3 en votre nom, puis de charger les données stockées dans ce compartiment dans un cluster Amazon Redshift. Pour plus d'informations, consultez Création d'un rôle pour déléguer des autorisations à un service AWS dans le IAM Guide de l'utilisateur.

  - Applications qui s'exécutent sur Amazon EC2 – Vous pouvez utiliser un rôle IAM pour gérer des informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et effectuent des demandes d'API AWS CLI ou AWS. Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un rôle AWS à une instance EC2 et le rendre disponible à toutes les applications associées, vous pouvez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le IAM Guide de l'utilisateur.

Contrôle d'accès

Vous pouvez avoir des informations d'identification valides pour authentifier vos demandes, mais à moins d'avoir les autorisations requises, vous ne pouvez pas créer de ressources AWS SSO ni accéder à de

telles ressources. Par exemple, vous devez disposer d'autorisations pour créer un annuaire connecté AWS SSO.

Les sections suivantes décrivent comment gérer les autorisations pour AWS SSO. Nous vous recommandons de commencer par lire la présentation.

Présentation de la gestion des autorisations d'accès à vos ressources AWS SSO

Chaque ressource AWS appartient à un compte AWS et les autorisations permettant de créer des ressources et d'y accéder sont régies par les stratégies d'autorisation. Un compte administrateur peut attacher des stratégies d'autorisations à des identités IAM (c'est-à-dire des utilisateurs, des groupes et des rôles). Certains services (comme AWS Lambda) prennent également en charge l'attachement de stratégies d'autorisation 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 IAM Guide de l'utilisateur.

Lorsque vous accordez des autorisations, vous décidez qui doit les obtenir, à quelles ressources ces autorisations s'appliquent et les actions spécifiques que vous souhaitez autoriser sur ces ressources.

Rubriques

Ressources et opérations AWS SSO

Dans AWS SSO, les ressources principales sont les instances d'application, les profils et les jeux d'autorisations.

Présentation de la propriété des ressources

Un propriétaire de ressource est le compte AWS qui a créé une ressource. En d'autres termes, le propriétaire de la ressource est le compte AWS de l'entité principale (le compte, un utilisateur IAM ou un rôle IAM) qui authentifie la demande qui crée la ressource. Les exemples suivants illustrent comment cela fonctionne :

- Si l'utilisateur racine du compte AWS crée une ressource AWS SSO, par exemple une instance d'application ou un jeu d'autorisations, votre compte AWS est le propriétaire de cette ressource.

- Si vous créez un utilisateur IAM dans votre compte AWS et autorisez cet utilisateur à créer une ressource AWS SSO il peut alors créer une ressource AWS SSO. Toutefois, votre compte AWS auquel appartient l'utilisateur, détient ces ressources .
- Si vous créez un rôle IAM dans votre compte AWS et que vous l'autorisez à créer des ressources AWS SSO, toute personne capable d'assumer le rôle peut créer des ressources AWS SSO. Toutefois, votre compte AWS, auquel ce rôle appartient, reste le propriétaire des ressources AWS SSO.

Gestion de l'accès aux ressources

Une stratégie d'autorisation décrit qui a accès à quoi. La section suivante explique les options disponibles pour créer des stratégies d'autorisation.

> Note
>
> Cette section décrit l'utilisation d'IAM dans le contexte d'AWS SSO. Elle ne fournit pas d'informations détaillées sur le service IAM. Pour accéder à la documentation complète de IAM, consultez Qu'est-ce qu'IAM ? dans le IAM Guide de l'utilisateur. Pour plus d'informations sur la syntaxe des stratégies IAM et des descriptions, consultez Référence de stratégie AWS IAM dans le IAM Guide de l'utilisateur.

Les stratégies qui sont associés à une identité IAM sont appelées des stratégies basées sur l'identité (stratégies IAM). Les stratégies qui sont associées à une ressource sont appelées des stratégies basées sur les ressources. AWS SSO prend en charge uniquement les stratégies basées sur une identité (stratégies IAM).

Rubriques

Stratégies basées sur une identité (stratégies IAM)

Vous pouvez attacher des stratégies à des identités IAM. Par exemple, vous pouvez effectuer les opérations suivantes :

- Attacher une stratégie d'autorisations à un utilisateur ou à un groupe dans votre compte – Un administrateur de compte peut utiliser une stratégie d'autorisations associée à un utilisateur spécifique pour autoriser cet utilisateur à ajouter une ressource AWS SSO, par exemple une nouvelle application.
- Attacher une stratégie d'autorisation à un rôle (accorder des autorisations entre comptes) – Vous pouvez attacher une stratégie d'autorisation basée sur une identité à un rôle IAM pour accorder des autorisations entre comptes. Par exemple, l'administrateur du Compte A peut créer un rôle afin d'accorder des autorisations inter-comptes à un autre compte AWS (par exemple, le Compte B) ou à un service AWS comme suit :
  1. L'administrateur du compte A crée un rôle IAM et attache une stratégie d'autorisations au rôle qui accorde des autorisations sur les ressources dans le compte A.
  2. L'administrateur du Compte A attache une stratégie d'approbation au rôle identifiant le Compte B comme mandataire pouvant assumer ce rôle.
  3. L'administrateur du Compte B peut alors déléguer des autorisations pour assumer le rôle à tous les utilisateurs figurant dans le Compte B. Cela autorise les utilisateurs du Compte B à créer des ressources ou à y accéder dans le Compte A. Le mandataire dans la stratégie d'approbation peut également être un mandataire de service AWS si vous souhaitez accorder à un service AWS des autorisations pour assumer ce rôle.

  Pour plus d'informations sur l'utilisation d'IAM pour déléguer des autorisations, consultez Gestion d'accès dans le IAM Guide de l'utilisateur.

La stratégie d'autorisation suivante accorde des autorisations à un utilisateur lui permettant d'exécuter toutes les actions commençant par `List`. Ces actions présentent des informations sur une ressource AWS SSO, par exemple une instance d'application ou un jeu d'autorisations. Notez que le caractère générique (*) figurant dans l'élément `Resource` indique que les actions sont autorisées pour toutes les ressources AWS SSO détenues par le compte.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"sso:List*",
         "Resource":"*"
      }
   ]
}
```

Pour plus d'informations sur l'utilisation des stratégies basées sur une identité avec AWS SSO, consultez Utilisation des stratégies basées sur une identité (stratégies IAM) pour AWS SSO (p. 34). Pour plus d'informations sur les utilisateurs, les groupes, les rôles et les autorisations, consultez Identités (utilisateurs, groupes et rôles) dans le manuel IAM Guide de l'utilisateur.

Stratégies basées sur une ressource

D'autres services, tels que Amazon S3, prennent également en charge les stratégies d'autorisation basées sur une ressource. Par exemple, vous pouvez attacher une stratégie à un compartiment S3 pour gérer les autorisations d'accès à ce compartiment. AWS SSO ne prend pas en charge les stratégies basées sur une ressource.

Spécification des éléments d'une stratégie : actions, effets, ressources et mandataires

Pour chaque ressource AWS SSO (voir Ressources et opérations AWS SSO (p. 31)), le service définit un ensemble d'opérations d'API. Pour accorder des autorisations pour ces opérations d'API, AWS SSO définit un ensemble d'actions que vous pouvez spécifier dans une stratégie. Notez que l'exécution d'une opération d'API peut exiger des autorisations pour plusieurs actions.

Voici les éléments de base d'une stratégie :

- Ressource – Dans une stratégie, vous utilisez un Amazon Resource Name (ARN) pour identifier la ressource à laquelle la stratégie s'applique. Pour des ressources AWS SSO, vous devez toujours utiliser le caractère générique (*) dans les stratégies IAM. Pour plus d'informations, consultez Ressources et opérations AWS SSO (p. 31).
- Action – Vous utilisez des mots clés d'action pour identifier les opérations de ressource que vous voulez accorder ou refuser. Par exemple, l'autorisation `sso:DescribePermissionsPolicies` permet à l'utilisateur d'effectuer l'opération AWS SSO `DescribePermissionsPolicies`.
- Effet – Vous spécifiez l'effet produit lorsque l'utilisateur demande l'action spécifique—qui peut être un accord 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 stratégie différente accorde l'accès.
- Mandataire – Dans les stratégies basées sur une identité (stratégies IAM), l'utilisateur auquel la stratégie est attachée est le mandataire implicite. Pour les stratégies 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 stratégies basées sur une ressource). AWS SSO ne prend pas en charge les stratégies basées sur une ressource.

Pour en savoir plus sur la syntaxe des stratégies IAM et obtenir des descriptions, consultez Référence de stratégie AWS IAM dans le IAM Guide de l'utilisateur.

Spécification de conditions dans une stratégie

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 stratégie après seulement une date spécifique. Pour plus d'informations sur la spécification de conditions dans un langage de stratégie, consultez Condition dans le IAM Guide de l'utilisateur.

Pour exprimer des conditions, vous utilisez des clés de condition prédéfinies. Il n'existe pas de clés de condition spécifiques à AWS SSO. Il existe, toutefois, des clés de condition AWS que vous pouvez utiliser selon vos besoins. Pour une liste complète des clés AWS, consultez Clés de condition disponibles dans le IAM Guide de l'utilisateur.

Utilisation des stratégies basées sur une identité (stratégies IAM) pour AWS SSO

Cette rubrique fournit des exemples de stratégies d'autorisations qu'un administrateur de compte peut attacher aux identités IAM (c'est-à-dire aux utilisateurs, groupes et rôles).

> Important
>
> Nous vous recommandons tout d'abord d'examiner les rubriques de présentation qui détaillent les concepts de base et les options disponibles pour gérer l'accès à vos ressources AWS SSO. Pour plus d'informations, consultez Présentation de la gestion des autorisations d'accès à vos ressources AWS SSO (p. 31).

Les sections de cette rubrique couvrent les sujets suivants :

Un exemple de stratégie d'autorisation est exposé ci-dessous.

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sso:CreateApplicationInstance",
        "sso:UpdateResponseConfig",
        "sso:UpdateResponseSchemaConfig",
        "sso:UpdateSecurityConfig",
        "sso:UpdateServiceProviderConfig",
        "sso:UpdateApplicationInstanceStatus",
        "sso:UpdateApplicationInstanceDisplay",
        "sso:CreateProfile",
        "sso:SetupTrust"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },

    {
      "Action" : [
```

```
        "organizations:xxx",
        "organizations:yyy"
       ],
      "Effect" : "Allow",
      "Resource" : "*"
    },

    {
      "Action" : [
        "ds:AuthorizeApplication"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

La stratégie comprend les éléments suivants :

- La première instruction accorde l'autorisation de gérer les associations de profils aux utilisateurs et aux groupes dans votre annuaire. Elle accorde également l'autorisation de lire toutes les ressources AWS SSO.
- La deuxième instruction accorde les autorisations de recherche de l'annuaire pour les utilisateurs et les groupes. Il est obligatoire de rechercher l'annuaire pour pouvoir créer des associations de profils.

La stratégie ne spécifie pas l'élément `Principal` car, dans une stratégie basée sur une identité, vous ne spécifiez pas le mandataire qui obtient l'autorisation. Quand vous attachez une stratégie à un utilisateur, l'utilisateur est le mandataire implicite. Lorsque vous attachez une stratégie d'autorisations à un rôle IAM, le mandataire identifié dans la stratégie d'approbation de ce rôle obtient les autorisations.

Autorisations requises pour utiliser la console AWS SSO

Pour qu'un utilisateur puisse utiliser la console AWS SSO, il doit avoir les autorisations répertoriées dans la stratégie précédente.

Si vous créez une stratégie IAM plus restrictive que les autorisations minimales requises, la console ne fonctionnera pas comme prévu pour les utilisateurs dotés de cette stratégie IAM.

Stratégies gérées par AWS (prédéfinies) pour AWS SSO

AWS est adapté à de nombreux cas d'utilisation courants et fournit des stratégies IAM autonomes qui sont créées et administrées par AWS. Les stratégies gérées octroient les autorisations requises dans les cas d'utilisation courants et vous évitent d'avoir à réfléchir aux autorisations qui sont requises. Pour plus d'informations, consultez Stratégies gérées par AWS dans le IAM Guide de l'utilisateur.

Exemples de stratégies gérées par le client

Dans cette section, vous trouverez des exemples de stratégies utilisateur qui accordent des autorisations pour diverses actions AWS SSO.

Exemples

- Exemple 1 : Autoriser un utilisateur à configurer et activer AWS SSO (p. 36)
- Exemple 2 : Autoriser un utilisateur à gérer votre annuaire connecté AWS SSO (p. 36)

Exemple 1 : Autoriser un utilisateur à configurer et activer AWS SSO

La stratégie d'autorisations suivante accorde les autorisations permettant à un utilisateur d'ouvrir la console AWS SSO et d'activer le service. Pour cela, des autorisations telles que celles accordées au compte principal AWS Organizations sont également requises.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
                sso:StartSSO,
                sso:GetSSOStatus
                  ],
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action": [
                organizations:DescribeAccount,
                organizations:EnableAWSServiceAccess
                  ],
         "Resource":"*"

      }
   ]
}
```

Exemple 2 : Autoriser un utilisateur à gérer votre annuaire connecté AWS SSO

La stratégie d'autorisations suivante accorde à un utilisateur les autorisations nécessaires pour gérer votre annuaire connecté.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
                sso:AssociateDirectory,
                sso:DisassociateDirectory,
                sso:ListDirectoryAssociations,
                sso:UpdateDirectoryAssociation
                  ],
         "Resource":"*"
      },
```

```
      {
         "Effect":"Allow",
         "Action": [
                ds:DescribeDirectories
                  ],
         "Resource":"*"
      }
   ]
}
```

Exemple 3 : Autoriser un utilisateur à gérer des applications dans AWS SSO

La stratégie d'autorisations suivante accorde les autorisations permettant à un utilisateur de créer et gérer des instances, profils et certificats d'application dans la console AWS SSO.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
                sso:ListApplicationTemplates,
                sso:GetApplicationTemplate
                sso:ListApplicationInstances,
                sso:GetApplicationInstance,
                sso:CreateApplicationInstance,
                sso:UpdateApplicationInstanceStatus,
                sso:UpdateApplicationInstanceDisplayData,
                sso:UpdateApplicationInstanceServiceProviderConfiguration,
                sso:UpdateApplicationInstanceResponseConfiguration,
                sso:UpdateApplicationInstanceResponseSchemaConfiguration,
                sso:UpdateApplicationInstanceSecurityConfiguration,
                sso:DeleteApplicationInstance,
                sso:ImportApplicationInstanceServiceProviderMetadata,
                sso:CreateProfile,
                sso:UpdateProfile,
                sso:DeleteProfile,
                sso:GetProfile,
                sso:ListProfiles,
                sso:ListApplicationInstanceCertificates,
                sso:CreateApplicationInstanceCertificate,
                sso:UpdateApplicationInstanceActiveCertificate,
                sso:DeleteApplicationInstanceCertificate
                  ],
         "Resource":"*"
      }
   ]
}
```

Exemple 4 : Autoriser un utilisateur à gérer les autorisations pour vos comptes AWS dans AWS SSO

La stratégie d'autorisations suivante accorde les autorisations permettant à un utilisateur de créer et gérer des jeux d'autorisations pour vos comptes AWS dans la console AWS SSO.

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

```
         "Effect":"Allow",
         "Action": [
                sso:ListApplicationInstances,
                sso:GetApplicationInstance,
                sso:CreateApplicationInstance,
                sso:UpdateApplicationInstanceStatus,
                sso:UpdateApplicationInstanceDisplayData,
                sso:UpdateApplicationInstanceServiceProviderConfiguration,
                sso:UpdateApplicationInstanceResponseConfiguration,
                sso:UpdateApplicationInstanceResponseSchemaConfiguration,
                sso:UpdateApplicationInstanceSecurityConfiguration,
                sso:DeleteApplicationInstance,
                sso:ImportApplicationInstanceServiceProviderMetadata,
                sso:CreateProfile,
                sso:UpdateProfile,
                sso:DeleteProfile,
                sso:GetProfile,
                sso:ListProfiles,
                sso:ListApplicationInstanceCertificates,
                sso:CreateApplicationInstanceCertificate,
                sso:UpdateApplicationInstanceActiveCertificate,
                sso:DeleteApplicationInstanceCertificate,
                sso:CreatePermissionSet,
                sso:GetPermissionSet,
                sso:ListPermissionSets,
                sso:DeletePermissionSet,
                sso:PutPermissionsPolicy,
                sso:DeletePermissionsPolicy,
                sso:DescribePermissionsPolicies,
                sso:GetTrust,
                sso:CreateTrust,
                sso:UpdateTrust,
                sso:DeleteTrust
                  ],
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action": [
                organizations:DescribeOrganization
                  ],
         "Resource":"*"
      }
   ]
}
```

Exemple 5 : Autoriser un utilisateur à gérer l'accès à vos applications dans AWS SSO

La stratégie d'autorisations suivante accorde les autorisations permettant à un utilisateur de gérer les personnes qui peuvent accéder à vos applications dans la console AWS SSO.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
                sso:ListApplicationInstances,
                sso:ListProfileAssociations,
                sso:AssociateProfile,
                sso:DisassociateProfile
                  ],
```

```
            "Resource":"*"
        },
        {
            "Effect":"Allow",
            "Action": [
                   ds:DescribeDirectories
                     ],
            "Resource":"*"
        }
    ]
}
```

Exemple 6 : Autoriser un utilisateur à rechercher les applications cloud préintégrées à AWS SSO

La stratégie d'autorisations suivante accorde les autorisations permettant à un utilisateur de rechercher, à l'aide de l'assistant d'ajout d'une application, les applications cloud préintégrées à AWS SSO.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
                sso:ListApplicationTemplates,
                sso:GetApplicationTemplate
                  ],
         "Resource":"*"
      }
   ]
}
```

Exemple 7 : Autoriser un utilisateur à ajouter des utilisateurs et des groupes dans AWS SSO

La stratégie d'autorisations suivante accorde les autorisations permettant à un utilisateur d'ouvrir la console AWS SSO et d'ajouter des utilisateurs et des groupes dans l'annuaire fourni par défaut par AWS SSO.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
                "sso-directory:*"
                  ],
         "Resource":"*"
      }
   ]
}
```

Utilisation des rôles liés à un service pour AWS SSO

AWS Single Sign-On utilise des rôles liés à un service AWS Identity and Access Management (IAM). Un rôle lié à un service est un type unique de rôle IAM lié directement à AWS SSO. Ce rôle est prédéfini par

AWS SSO et comprend toutes les autorisations nécessaires au service pour appeler d'autres services AWS en votre nom. Pour plus d'informations, consultez Rôles liés à un service (p. 21).

Un rôle lié à un service permet d'utiliser AWS SSO plus facilement, car vous n'avez pas besoin d'ajouter manuellement les autorisations requises. AWS SSO définit les autorisations de son rôle lié à un service et, sauf définition contraire, seul AWS SSO peut endosser son rôle. Les autorisations définies comprennent la stratégie d'approbation et la stratégie d'autorisation. De plus, cette stratégie 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 à un service, consultez Services AWS qui fonctionnent avec IAM et recherchez les services qui comportent Oui dans la colonne Rôle lié à un service. Choisissez un Oui ayant un lien permettant de consulter la documentation du rôle lié à un service, pour ce service.

Autorisations des rôles liés à un service pour AWS SSO

AWS SSO utilise le rôle lié à un service intitulé AWSServiceRoleForSSO pour accorder les autorisations AWS SSO de gestion des ressources AWS, notamment les rôles et stratégies IAM, et l'IdP SAML, en votre nom.

Le rôle lié à un service AWSServiceRoleForSSO approuve les services suivants pour endosser le rôle :

- `AWS SSO`

La stratégie d'autorisations du rôle lié à un service AWSServiceRoleForSSO permet à AWS SSO d'effectuer les actions suivantes sur les rôles dans le chemin « /aws-reserved/sso.amazonaws.com/ » et avec le préfixe de nom « AWSReservedSSO_ » :

- `iam:AttachRolePolicy`
- `iam:CreateRole`
- `iam:DeleteRole`
- `iam:DeleteRolePolicy`
- `iam:DetachRolePolicy`
- `iam:GetRole`
- `iam:ListRolePolicies`
- `iam:PutRolePolicy`
- `iam:ListAttachedRolePolicies`

La stratégie d'autorisations du rôle lié à un service AWSServiceRoleForSSO permet à AWS SSO d'effectuer les actions suivantes sur les fournisseurs SAML avec le préfixe de nom « AWSSSO_ » :

- `iam:CreateSAMLProvider`
- `iam:GetSAMLProvider`
- `iam:UpdateSAMLProvider`
- `iam:DeleteSAMLProvider`

La stratégie d'autorisations du rôle lié au service AWSServiceRoleForSSO permet à AWS SSO d'effectuer les actions suivantes sur toutes les organisations :

- `organizations:DescribeAccount`
- `organizations:DescribeOrganization`

- `organizations:ListAccounts`

La stratégie d'autorisations du rôle lié au service AWSServiceRoleForSSO permet à AWS SSO d'effectuer les actions suivantes sur tous les rôles IAM (*) :

- `iam:listRoles`

La stratégie des autorisations du rôle lié à un service AWSServiceRoleForSSO permet à AWS SSO d'effectuer les actions suivantes sur arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/AWSServiceRoleForSSO :

- `iam:GetServiceLinkedRoleDeletionStatus`
- `iam:DeleteServiceLinkedRole`

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, groupe ou 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 IAM Guide de l'utilisateur.

Création d'un rôle lié à un service pour AWS SSO

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. When a user who is signed in with the AWS organization’s master account assigns access to an AWS account for the first time, AWS SSO creates the service-linked role automatically in that AWS account.

> Important
>
> Si vous utilisiez AWS SSO avant December 7, 2017, quand il commençait à prendre en charge les rôles liés à un service, AWS SSO créait le rôle AWSServiceRoleForSSO dans votre compte. Pour en savoir plus, consultez 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 AWS SSO

AWS SSO ne vous permet pas de modifier le rôle lié à un service AWSServiceRoleForSSO. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas modifier le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide de IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le IAM Guide de l'utilisateur.

Suppression d'un rôle lié à un service pour AWS SSO

Vous n'avez pas besoin de supprimer manuellement le rôle AWSServiceRoleForSSO. When an AWS account is removed from an AWS organization, AWS SSO automatically cleans up the resources and deletes the service-linked role from that AWS account.

Vous pouvez également utiliser la console IAM, l'interface de ligne de commande 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 AWS SSO utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression peut échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer les ressources AWS SSO utilisées par le service AWSServiceRoleForSSO

1. Suppression d'un accès utilisateur (p. 18) pour tous les utilisateurs et groupes qui ont accès au compte AWS.
2. Suppression de jeux d'autorisations (p. 20) que vous avez associé au compte AWS.
3. Suppression du fournisseur d'identité IAM (p. 21) pour supprimer la relation d'approbation entre AWS SSO et le compte AWS.

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, le CLI IAM ou l'API IAM pour supprimer le rôle lié à un service AWSServiceRoleForSSO. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le IAM Guide de l'utilisateur.

Utilisation du portail utilisateur

Votre portail utilisateur vous fournit un accès par authentification unique à tous vos comptes AWS et à la plupart des applications cloud les plus couramment utilisées, comme Office 365, Concur, Salesforce, et bien d'autres. Vous pouvez l'utiliser pour lancer rapidement plusieurs applications en choisissant le compte ou l'icône de l'application AWS dans le portail. La présence d'icônes dans votre portail signifie qu'un administrateur ou un employé désigné du service d'assistance de votre entreprise vous a accordé l'accès à ces comptes ou applications AWS. Cela signifie également que vous pouvez accéder à tous ces comptes ou applications depuis le portail sans invites de connexion supplémentaires.

Contactez votre administrateur ou votre service d'assistance pour lui demander un accès supplémentaire dans les cas suivants :

- Vous avez besoin d'accéder à un compte ou une application AWS que vous ne voyez pas.
- L'accès que vous avez à une application ou un compte donné n'est pas ce que vous avez prévu.

Rubriques

Conseils d'utilisation du portail

Comme toute application ou tout outil commercial utilisé quotidiennement, le portail utilisateur peut ne pas fonctionner comme prévu. Dans ce cas, essayez d'appliquer les conseils suivants :

- Vous devrez parfois vous déconnecter du portail utilisateur, puis vous y reconnecter. 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.
- Après vous être connecté au portail utilisateur, vous pouvez ouvrir l'une des applications répertoriées en choisissant son icône. Une fois que vous avez terminé d'utiliser une application, vous pouvez la fermer ou vous déconnecter du portail utilisateur. Si vous vous contentez de fermer l'application, vous n'êtes pas déconnecté du portail utilisateur. Toutes les autres applications que vous avez ouvertes dans le portail utilisateur restent ouvertes et en cours d'exécution.
- Avant de pouvoir vous connecter sous l'identité d'un autre utilisateur dans le portail utilisateur, vous devez commencer par vous déconnecter. Lorsque vous vous déconnectez du portail utilisateur, toutes vos informations d'identification sont supprimées de la session du navigateur.

Comment accepter l'invitation à rejoindre AWS SSO

Si c'est la première fois que vous vous connectez au portail utilisateur, consultez dans votre e-mail les instructions sur comment activer votre compte.

Pour réactiver votre compte

1. Selon l'e-mail que vous avez reçu de votre entreprise, choisissez l'une des méthodes suivantes afin d'activer votre compte pour pouvoir commencer à utiliser le portail d'utilisateur.

   a. Si vous avez reçu un e-mail avec l'objet Invitation to join AWS Single Sign-On (Invitation à rejoindre AWS SSO), ouvrez-le et choisissez Accept invitation (Accepter l'invitation), ce qui vous permet d'accéder à la page Single Sign-On (Authentification unique). Sur cette page, vous spécifiez un mot de passe que vous utiliserez chaque fois que vous vous connecterez sur au portail. Une fois que vous avez entré un mot de passe et que vous l'avez confirmé, choisissez Update User (Mettre à jour l'utilisateur).

   b. Si vous avez reçu un e-mail du support informatique ou de l'administrateur informatique de votre entreprise, suivez les instructions fournies pour activer votre compte.

2. Une fois que vous avez activé votre compte en fournissant un nouveau mot de passe, le portail utilisateur vous connecte automatiquement. Si ce ne se produit pas, vous pouvez vous connecter manuellement au portail utilisateur en utilisant les instructions fournies à l'étape suivante.

Comment se connecter au portail utilisateur

À ce stade, vous devriez avoir reçu une URL de connexion au portail utilisateur envoyée par un administrateur ou un employé du service d'assistance. Une fois que vous l'avez reçue, vous pouvez procéder comme suit pour vous connecter au portail.

Pour vous connecter au portail utilisateur

1. Dans la fenêtre de votre navigateur, collez l'URL de connexion qui vous a été fournie. Appuyez ensuite sur Entrée. Nous vous recommandons de placer un signet sur ce lien pour pouvoir le réutiliser facilement.
2. Connectez-vous avec votre nom d'utilisateur et votre mot de passe standard.
3. Une fois connecté, vous pouvez accéder à tout compte ou application AWS qui s'affiche dans le portail. Il vous suffit de choisir une icône.

Comment se déconnecter du portail utilisateur

Lorsque vous vous déconnectez du portail utilisateur, vos informations d'identification sont entièrement supprimées de la session du navigateur.

Note

Pour vous connecter sous l'identité d'un autre utilisateur, vous devez commencer par vous déconnecter.

Pour se déconnecter du portail utilisateur

- Dans le portail utilisateur, choisissez Sign out (Déconnexion) dans le coin supérieur droit du portail.

Comment rechercher un compte ou une application AWS

Si votre liste d'applications ou de comptes AWS est trop longue, ce qui ne vous permet pas de trouver facilement ce dont vous avez besoin, vous pouvez utiliser la zone Search (Rechercher).

Pour rechercher un compte AWS ou une application dans le portail utilisateur

1. Après vous être connecté au portail, choisissez la zone Search (Rechercher).
2. Saisissez le nom de l'application. Appuyez ensuite sur Entrée.

Comment réinitialiser votre mot de passe

De temps en temps, vous pouvez avoir besoin de réinitialiser votre mot de passe, en fonction des stratégies de votre entreprise.

Pour réinitialiser votre mot de passe

1. Ouvrez un navigateur et allez à la page de connexion de votre portail utilisateur.
2. Sous le bouton Sign-In (Connexion), choisissez Forgot Password? (Mot de passe oublié ?).
3. Indiquez votre Username (Nom d'utilisateur) et saisissez les caractères de l'image fournie afin de confirmer que vous n'êtes pas un robot. Choisissez ensuite Recover Password (Récupérer le mot de passe). Vous recevez alors un e-mail avec l'objet AWS Directory Service Reset Password Request (Demande de réinitialisation du mot de passe AWS Directory Service).
4. Une fois que vous avez reçu l'e-mail, choisissez Reset Password (Réinitialiser le mot de passe).
5. Sur la page Single Sign-On (Authentification unique), vous devez spécifier un nouveau mot de passe pour le portail. Une fois que vous avez entré un mot de passe et que vous l'avez confirmé, choisissez Reset Password (Réinitialiser le mot de passe).

Comment obtenir les informations d'identification d'un rôle IAM pour les utiliser avec l'accès par interface de ligne de commande à un compte AWS

Utilisez cette procédure dans le portail utilisateur lorsque vous avez besoin d'informations d'identification de sécurité temporaires pour accéder à court terme aux ressources d'un compte AWS à l'aide de l'AWS CLI. Le portail utilisateur permet de sélectionner rapidement un compte AWS et d'obtenir les informations d'identification temporaires correspondant à un rôle IAM. Vous pouvez ensuite copier la syntaxe d'interface de ligne de commande nécessaire (avec toutes les informations d'identification) et la coller dans votre invite de commande d'AWS CLI.

Par défaut, les informations d'identification récupérées dans le portail utilisateur sont valides pendant 1 heure. Vous pouvez modifier cette valeur jusqu'à 12 heures. Une fois que vous avez terminé cette procédure, vous pouvez exécuter toute commande d'AWS CLI (à laquelle votre administrateur vous a donné accès) jusqu'à l'expiration de ces informations d'identification temporaires.

> Note
>
> Avant d'entamer cette procédure, vous devez commencer par installer l'AWS CLI. Pour obtenir les instructions nécessaires, consultez Installation de l'interface de ligne de commande AWS.

Comment obtenir les informations d'identification temporaires d'un rôle IAM pour accéder à un compte AWS à l'aide de l'interface de ligne de commande

1. Après vous être connecté au portail, choisissez l'icône AWS Accounts (Comptes AWS) pour développer la liste des comptes.

2. Choisissez le compte AWS à partir duquel vous souhaitez récupérer les informations d'identification d'accès. Ensuite, en regard du nom du rôle IAM (par exemple Administrator (Administrateur)), choisissez Command line or programmatic access (Ligne de commande ou accès par programme).
3. Dans la boîte de dialogue Get credentials (Obtenir des informations d'identification), choisissez MacOS and Linux (MacOS et Linux) ou Windows, selon le système d'exploitation dans lequel vous prévoyez d'utiliser l'invite de commande de l'interface de ligne de commande.
4. Selon la manière dont vous souhaitez utiliser les informations d'identification temporaires, choisissez une ou plusieurs des options suivantes :

   - Pour exécuter des commandes à partir de l'AWS CLI dans le compte AWS sélectionné, sous Option 1: Set AWS environment variables (Option 1 : Définir les variables d'environnement AWS), arrêtez-vous sur les commandes. Choisissez ensuite Copy (Copier). Collez les commandes dans la fenêtre de terminal d'interface de ligne de commande et appuyez sur Entrée pour définir les variables d'environnement nécessaires.
   - Pour exécuter des commandes à partir de plusieurs invites de commande dans le même compte AWS, sous Option 2: Add a profile to your AWS credentials file (Option 2 : Ajouter un profil à votre fichier d'informations d'identification AWS), arrêtez-vous sur les commandes. Choisissez ensuite Copy (Copier). Collez les commandes dans votre fichier d'informations d'identification AWS pour configurer un nouveau profil nommé. Pour plus d'informations, consultez Fichiers de configuration et d'informations d'identification dans le Guide de l'utilisateur de l'AWS CLI. En modifiant les fichiers d'informations d'identification de cette manière, vous activez l'option `--profile` dans votre commande d'AWS CLI pour pouvoir utiliser ces informations d'identification. Cela affecte toutes les invites de commande qui utilisent le même fichier d'informations d'identification.
   - Si vous avez besoin d'accéder aux ressources AWS à partir d'un client de service AWS, sous Option 3: Use individual values in your AWS service client (Option 3 : Utiliser des valeurs individuelles dans votre client de service AWS), choisissez Copy (Copier) en regard des commandes que vous devez utiliser. Pour plus d'informations, consultez Obtention d'informations d'identification temporaires avec AWS STS dans le Guide de l'utilisateur de l'interface de ligne de commande AWS ou consultez Outils pour Amazon Web Services.
5. Continuez à utiliser l'AWS CLI selon vos besoins pour votre compte AWS jusqu'à l'expiration des informations d'identification.

Journalisation des appels d'API AWS SSO avec AWS CloudTrail

AWS SSO est intégré à AWS CloudTrail, service qui enregistre les actions effectuées par un utilisateur, un rôle ou un service AWS dans AWS SSO. Si vous créez un journal de suivi, vous pouvez diffuser en continu les événements CloudTrail dans un compartiment Amazon S3, Amazon CloudWatch Logs et Amazon CloudWatch Events. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été envoyée à AWS SSO, l'adresse IP source à partir de laquelle la demande a été effectuée, l'auteur de la demande et la date de la demande, ainsi que d'autres informations.

Pour en savoir plus sur CloudTrail, consultez AWS CloudTrail User Guide.

Informations AWS SSO dans CloudTrail

CloudTrail est activé sur votre compte AWS lorsque vous créez le compte. Lorsqu'une activité a lieu dans AWS SSO, cette activité est enregistrée dans un événement CloudTrail avec d'autres événements de services AWS dans Event history (Historique des événements). Vous pouvez afficher, rechercher et télécharger les événements récents dans votre compte AWS. Pour plus d'informations, consultez Affichage des événements avec l'historique des événements CloudTrail.

Pour un enregistrement continu des événements dans votre compte AWS, y compris les événements pour AWS SSO, créez un journal de suivi. Une journal de suivi permet à CloudTrail de livrer les fichiers journaux dans 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 de suivi consigne les événements de toutes les régions dans la partition AWS et livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. En outre, vous pouvez configurer d'autres services AWS pour analyser plus en profondeur les données d'événement collectées dans les journaux CloudTrail et agir sur celles-ci. Pour plus d'informations, consultez les ressources suivantes :

- Présentation de la création d'un journal de suivi
- Intégrations et services pris en charge par CloudTrail
- Configuration des Notifications de Amazon SNS pour CloudTrail
- Réception de fichiers journaux CloudTrail de plusieurs régions et Réception de fichiers journaux CloudTrail de plusieurs comptes

Lorsque la journalisation CloudTrail est activée dans votre compte AWS, les appels d'API passés aux actions AWS SSO sont suivis dans les fichiers journaux. Les enregistrements AWS SSO sont écrits avec d'autres enregistrements de service AWS dans un fichier journal. CloudTrail détermine quand créer un fichier et y consigner des données en fonction d'une période et d'une taille de fichier.

Les actions suivantes sont prises en charge :

- `AssociateDirectory`
- `AssociateProfile`
- `CreateApplicationInstance`
- `CreateApplicationInstanceCertificate`
- `CreatePermissionSet`

- `CreateProfile`
- `DeleteApplicationInstance`
- `DeleteApplicationInstanceCertificate`
- `DeletePermissionsPolicy`
- `DeletePermissionSet`
- `DeleteProfile`
- `DescribePermissionsPolicies`
- `DisassociateDirectory`
- `DisassociateProfile`
- `GetApplicationInstance`
- `GetApplicationTemplate`
- `GetPermissionSet`
- `GetSSOStatus`
- `ImportApplicationInstanceServiceProviderMetadata`
- `ListApplicationInstances`
- `ListApplicationInstanceCertificates`
- `ListApplicationTemplates`
- `ListDirectoryAssociations`
- `ListPermissionSets`
- `ListProfileAssociations`
- `ListProfiles`
- `PutPermissionsPolicy`
- `StartSSO`
- `UpdateApplicationInstanceActiveCertificate`
- `UpdateApplicationInstanceDisplayData`
- `UpdateApplicationInstanceServiceProviderConfiguration`
- `UpdateApplicationInstanceStatus`
- `UpdateApplicationInstanceResponseConfiguration`
- `UpdateApplicationInstanceResponseSchemaConfiguration`
- `UpdateApplicationInstanceSecurityConfiguration`
- `UpdateDirectoryAssociation`
- `UpdateProfile`

Chaque entrée du journal contient des informations sur la personne qui a généré la demande. Les informations d'identité figurant dans le journal vous aident à déterminer si la demande a été effectuée par l'utilisateur racine d'un compte AWS ou avec les informations d'identification d'un utilisateur IAM. Elles vous indiquent également si la demande a été effectuée avec des informations d'identification de sécurité temporaires correspondant à un rôle ou un utilisateur fédéré, ou par un autre service AWS. Pour plus d'informations, consultez la section Élément userIdentity CloudTrail.

Vous pouvez créez un journal de suivi et stocker vos fichiers journaux dans votre compartiment Amazon S3 aussi longtemps que vous le souhaitez. Vous pouvez également définir des règles de cycle de vie Amazon S3 pour archiver ou supprimer les fichiers journaux automatiquement. Par défaut, vos fichiers journaux sont chiffrés avec le chiffrement côté serveur (SSE) de Amazon S3.

Pour être averti de la remise des fichiers journaux, configurez CloudTrail pour qu'il publie des notifications Amazon SNS lorsque de nouveaux fichiers journaux sont remis. Pour plus d'informations, consultez Configuration des notifications Amazon SNS pour CloudTrail.

Vous pouvez également regrouper des fichiers journaux AWS SSO provenant de plusieurs régions AWS et de plusieurs comptes AWS dans un compartiment Amazon S3 unique. Pour plus d'informations, consultez Recevoir les fichiers journaux de CloudTrail de plusieurs régions et Recevoir les fichiers journaux de CloudTrail de plusieurs comptes.

Présentation des entrées des fichiers journaux AWS SSO

Un journal de suivi est une configuration qui active la livraison d'événements en tant que fichiers journaux à un compartiment Amazon S3 que vous spécifiez. Les fichiers journaux CloudTrail contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique à partir d'une source quelconque et comprend des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. Les fichiers journaux CloudTrail ne sont pas une pile ordonnée retraçant les appels d'API publics. Ils ne suivent donc aucun ordre précis.

L'exemple suivant montre une entrée de journal CloudTrail sur la console AWS SSO pour un administrateur (samadams@example.com) :


```
{
   "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 journal CloudTrail dans le portail utilisateur AWS SSO pour une action d'utilisateur final (bobsmith@example.com) :


```
{
   "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":"https://portal.sso.us-east-1.amazonaws.com/instance/appinstances",
         "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"
      }
   ]
}
```

Limites dans AWS SSO

Les tableaux suivants décrivent les limites au sein d'AWS SSO. Pour plus d'informations sur les limites qui peuvent être modifiées, consultez la section Limites de service AWS.

Limites de l'application

Ressource	Limite par défaut
Taille du fichier de certificats SAML du fournisseur de services (au format PEM)	2 Ko

Limites de compte AWS

Ressource	Limite par défaut
Nombre maximal de jeux d'autorisations dans AWS SSO	50
Nombre de jeux d'autorisations admis par compte AWS	20
Nombre de références à des stratégies gérées par AWS par jeu d'autorisations	10
Nombre de stratégies en ligne par jeu d'autorisations	1
Taille maximale de stratégie en ligne par jeu d'autorisations	10,000 bytes
Nombre de rôles IAM du compte AWS qui peuvent être réparés à la fois*	1
Nombre d'annuaires que vous pouvez avoir simultanément	1

* Les jeux d'autorisations sont alloués dans un compte AWS sous forme de rôles IAM. Pour plus d'informations, consultez Jeux d'autorisations (p. 6).

Limites de l'annuaire connecté

Ressource	Limite par défaut
Nombre de groupes Active Directory uniques qui peuvent être attribués *	50

Ressource	Limite par défaut
Nombre d'annuaires connectés que vous pouvez avoir simultanément	1

* Les utilisateurs appartenant à un annuaire Active Directory peuvent appartenir à plusieurs groupes d'annuaires. Dans AWS SSO, ils peuvent cependant avoir jusqu'à 50 de leurs groupes Active Directory attribués à l'utilisation des applications.

Limites d'annuaire AWS SSO

Ressource	Limite par défaut
Nombre maximum d'utilisateurs pris en charge dans AWS SSO	500
Nombre maximum de groupes pris en charge dans AWS SSO	100

Résolution des problèmes rencontrés avec AWS SSO

Les sections suivantes peuvent vous aider à résoudre certains problèmes courants que vous pouvez rencontrer lorsque vous configurez ou utilisez la console AWS SSO.

Je ne parviens pas à configurer correctement mon application cloud

Chaque fournisseur de services d'une application cloud préintégrée dans AWS SSO a son propre manuel d'instructions détaillé. Vous pouvez accéder à ce manuel à partir de l'onglet Configuration correspondant à cette application dans la console AWS SSO.

Si le problème est lié à la configuration de la relation d'approbation entre l'application du fournisseur de services et AWS SSO, veillez à consulter les étapes de résolution de ce problème dans le manuel d'instructions.

Je ne sais pas quelles sont les données de mon assertion SAML qui sont transmises au fournisseur de services

Procédez comme indiqué dans le portail utilisateur pour afficher les données de l'assertion SAML qui sont envoyées au fournisseur de services de l'application pour l'utilisateur actuellement connecté. Cette procédure affiche le contenu dans la fenêtre de navigateur avant de l'envoyer au fournisseur.

1. Après vous être connecté au portail, maintenez la touche Maj enfoncée, puis choisissez l'application.
2. Examinez les informations indiquées sur la page intitulée You are now in administrator mode (Vous êtes maintenant en mode administrateur).
3. Si elles sont correctes, vous pouvez choisir Send to (Envoyer à)<application> pour envoyer l'assertion au fournisseur de services et examiner le contenu de la réponse.

Historique du document

Le tableau suivant décrit la documentation de cette version d'AWS Single Sign-On.

- Dernière date de mise à jour de la documentation : 30 octobre 2018

update-history-change	update-history-description	update-history-date
Prise en charge de la durée de session sur les comptes AWS	Ajout de contenu sur la façon de définir la durée de session pour un compte AWS.	October 30, 2018
Nouvelle option pour utiliser un annuaire AWS SSO	Ajout de contenu pour choisir un annuaire AWS SSO ou une connexion à un annuaire AD existant.	October 17, 2018
Prise en charge de l'état de relais et de la durée de session sur les applications	Ajout de contenu sur le l'état de relais et la durée de session pour les applications cloud.	October 10, 2018
Prise en charge supplémentaire de nouvelles applications cloud	Ajout de 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.	August 3, 2018
Prise en charge de l'accès SSO aux comptes principaux	Ajout de contenu expliquant comment déléguer l'accès SSO à des utilisateurs dans un compte principal.	July 9, 2018
Prise en charge des nouvelles applications cloud	Les applications DocuSign, Keeper Security et SugarCRM ont été ajoutées au catalogue d'applications.	March 16, 2018
Obtention d'informations d'identification temporaires pour l'accès aux interfaces de ligne de commande	Des informations ont été ajoutées sur la façon d'obtenir des informations d'identification temporaires pour exécuter les commandes d'interface de ligne de commande AWS.	February 22, 2018

Nouveau guide	Il s'agit de la première version du guide de l'utilisateur AWS SSO.	December 7, 2017

Glossaire AWS

Pour la terminologie AWS la plus récente, consultez le Glossaire AWS dans le document AWS General Reference.