Guide de l’utilisateur

AWS Configuration

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Configuration: Guide de l’utilisateur

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques commerciales et la présentation commerciale d’Amazon ne peuvent pas être utilisées en relation avec un produit ou un service extérieur à Amazon, d’une manière susceptible d’entraîner une confusion chez les clients, ou d’une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d’Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Présentation 1
..... 1
..... 1
Terminologie 2
..... 2
Administrateur 2
Compte 2
Informations d'identification 2
Identifiants de l'entreprise 3
Profil 3
Utilisateur 3
Informations d'identification de l'utilisateur root 3
Code de vérification 4
AWS utilisateurs et informations d'identification 5
Utilisateur root 5
Utilisateur du centre d'identité IAM 6
Identité fédérée 6
Utilisateur IAM 6
AWS Utilisateur Builder ID 7
Prérequis et considérations 8
Compte AWS exigences 8
Considérations relatives à l'IAM Identity Center 9
Active Directory ou IdP externe 9
AWS Organizations 11
Rôles IAM 11
Pare-feux de nouvelle génération et passerelles Web sécurisées 11
Utilisation de plusieurs Comptes AWS 12
Partie 1 : Configuration d'un nouveau Compte AWS 14
Étape 1 : Ouvrez un AWS compte 14
Étape 2 : connectez-vous en tant qu'utilisateur root 16
Pour vous connecter en tant qu'utilisateur root 16
Étape 3 : activer le MFA pour votre utilisateur root Compte AWS 17
Partie 2 : Création d'un utilisateur administratif dans IAM Identity Center 18
Étape 1 : activer le centre d'identité IAM 18

Étape 2 : Choisissez votre source d'identité 19
Connectez Active Directory ou un autre IdP et spécifiez un utilisateur 20
Utiliser le répertoire par défaut et créer un utilisateur dans IAM Identity Center 23
Étape 3 : Création d'un ensemble d'autorisations administratives 24
Étape 4 : configurer Compte AWS l'accès pour un utilisateur administratif 25
Étape 5 : Connectez-vous au portail d' AWS accès avec vos informations d'identification administratives 26
Résolution des problèmes Compte AWS de création 29
Je n'ai pas reçu d'appel AWS pour vérifier mon nouveau compte 29
Je reçois une erreur concernant le « nombre maximum de tentatives infructueuses » lorsque j'essaie de vérifier mon identité Compte AWS par téléphone 30
Cela fait plus de 24 heures et mon compte n'est pas activé 30
..... xxxii

Présentation

Ce guide fournit des instructions pour créer un nouvel utilisateur administratif Compte AWS et configurer votre premier utilisateur conformément aux AWS IAM Identity Center meilleures pratiques de sécurité les plus récentes.

Un Compte AWS est nécessaire pour y accéder Services AWS et sert de deux fonctions de base :

- Conteneur — An Compte AWS est un conteneur pour toutes les AWS ressources que vous pouvez créer en tant que AWS client. Lorsque vous créez un bucket Amazon Simple Storage Service (Amazon S3) ou une base de données Amazon Relational Database Service (Amazon RDS) pour stocker vos données, ou une instance Amazon Elastic Compute Cloud (EC2Amazon) pour traiter vos données, vous créez une ressource dans votre compte. Chaque ressource est identifiée de manière unique par un Amazon Resource Name (ARN) qui inclut l'ID de compte du compte qui contient ou possède la ressource.
- Limite de sécurité — An Compte AWS est la limite de sécurité de base pour vos AWS ressources. Les ressources que vous créez dans votre compte ne sont accessibles qu'aux utilisateurs disposant d'informations d'identification pour ce même compte.

  Parmi les principales ressources que vous pouvez créer dans votre compte figurent les identités, telles que les utilisateurs et les rôles IAM, et les identités fédérées, telles que les utilisateurs de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web, de l'annuaire du centre d'identité IAM ou de tout autre utilisateur accédant à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Ces identités comportent des informations d'identification que quelqu'un peut utiliser pour se connecter ou s'authentifier AWS. Les identités ont également des politiques d'autorisation qui précisent ce que la personne qui s'est connectée est autorisée à faire avec les ressources du compte.

Terminologie

Amazon Web Services (AWS) utilise une terminologie courante pour décrire le processus de connexion. Nous vous recommandons de lire et de comprendre ces conditions.

Administrateur

Également appelé Compte AWS administrateur ou administrateur IAM. L'administrateur, généralement le personnel des technologies de l'information (TI), est une personne qui supervise un Compte AWS. Les administrateurs disposent d'un niveau d'autorisations supérieur à Compte AWS celui des autres membres de leur organisation. Les administrateurs établissent et mettent en œuvre les paramètres du Compte AWS. Ils créent également des utilisateurs IAM ou IAM Identity Center. L'administrateur fournit à ces utilisateurs leurs informations d'accès et une URL de connexion à laquelle se connecter AWS.

Compte

Une norme Compte AWS contient à la fois vos AWS ressources et les identités qui peuvent accéder à ces ressources. Les comptes sont associés à l'adresse e-mail et au mot de passe du propriétaire du compte.

Informations d'identification

Également appelés identifiants d'accès ou identifiants de sécurité. Les informations d'identification sont les informations que les utilisateurs fournissent AWS pour se connecter et accéder aux AWS ressources. Les informations d'identification peuvent inclure une adresse e-mail, un nom d'utilisateur, un mot de passe défini par l'utilisateur, un identifiant ou un alias de compte, un code de vérification et un code d'authentification multifactorielle à usage unique (MFA). Dans l'authentification et l'autorisation, un système utilise les informations d'identification pour identifier la personne qui effectue l'appel et pour autoriser ou pas l'accès demandé. Dans AWS, ces informations d'identification sont généralement l'ID de la clé d'accès et la clé d'accès secrète.

Pour plus d'informations sur les informations d'identification, voir Comprendre et obtenir vos AWS informations d'identification.

> **Note**
>
> Le type d'informations d'identification qu'un utilisateur doit soumettre dépend de son type d'utilisateur.

Identifiants de l'entreprise

Les informations d'identification fournies par les utilisateurs lorsqu'ils accèdent au réseau et aux ressources de leur entreprise. L'administrateur de votre entreprise peut configurer votre compte Compte AWS pour qu'il soit accessible avec les mêmes informations d'identification que celles que vous utilisez pour accéder au réseau et aux ressources de votre entreprise. Ces informations d'identification vous sont fournies par votre administrateur ou un employé du service d'assistance.

Profil

Lorsque vous vous inscrivez pour obtenir un AWS Builder ID, vous créez un profil. Votre profil inclut les informations de contact que vous avez fournies et la possibilité de gérer les appareils d'authentification multifactorielle (MFA) et les sessions actives. Vous pouvez également en savoir plus sur la confidentialité et la manière dont nous traitons vos données dans votre profil. Pour plus d'informations sur votre profil et son lien avec un Compte AWS, consultez AWS Builder ID et autres AWS informations d'identification.

Utilisateur

Un utilisateur est une personne ou une application associée à un compte qui effectue des appels d'API vers AWS des produits. Chaque utilisateur possède un nom unique Compte AWS et un ensemble d'informations de sécurité qui ne sont pas partagées avec d'autres utilisateurs. Ces informations d'identification sont distinctes des informations de sécurité pour Compte AWS. Chaque utilisateur est associé à un seul et unique utilisateur Compte AWS.

Informations d'identification de l'utilisateur root

Les informations d'identification de l'utilisateur root sont les mêmes AWS Management Console que celles utilisées pour se connecter à l'utilisateur root. Pour plus d'informations sur l'utilisateur root, consultez la section Utilisateur root.

Code de vérification

Un code de vérification vérifie votre identité lors du processus de connexion à l'aide de l'authentification multifactorielle (MFA). Les méthodes de livraison des codes de vérification varient. Ils peuvent être envoyés par SMS ou par e-mail. Consultez votre administrateur pour plus d'informations.

AWS utilisateurs et informations d'identification

Lorsque vous interagissez avec AWS, vous spécifiez vos informations de AWS sécurité pour vérifier qui vous êtes et si vous êtes autorisé à accéder aux ressources que vous demandez. AWS utilise des informations d'identification de sécurité pour authentifier et autoriser les demandes.

Par exemple, si vous souhaitez télécharger un fichier protégé à partir d'un compartiment Amazon Simple Storage Service (Amazon S3), vos informations d'identification doivent autoriser cet accès. Si vos informations d'identification indiquent que vous n'êtes pas autorisé à télécharger le fichier, AWS refuse votre demande. Cependant, les informations d'identification de sécurité ne sont pas requises pour télécharger des fichiers dans des compartiments Amazon S3 partagés publiquement.

Utilisateur root

Également appelé propriétaire du compte ou utilisateur root du compte. En tant qu'utilisateur root, vous avez un accès complet à tous les AWS services et ressources de votre Compte AWS. Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à tous les AWS services et ressources du compte. Cette identité est celle de l'utilisateur root du AWS compte. Vous pouvez vous connecter en AWS Management Consoletant qu'utilisateur root à l'aide de l'adresse e-mail et du mot de passe que vous avez utilisés pour créer le compte. Pour obtenir des instructions détaillées sur la procédure de connexion, voir Se connecter en AWS Management Console tant qu'utilisateur root.

> **Important**
>
> Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur racine, consultez Tâches nécessitant des informations d'identification d'utilisateur racine dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les identités IAM, y compris l'utilisateur root, consultez Identités IAM (utilisateurs, groupes d'utilisateurs et rôles).

Utilisateur du centre d'identité IAM

Un utilisateur de l'IAM Identity Center se connecte via le portail AWS d'accès. Le portail AWS d'accès ou l'URL de connexion spécifique est fourni par votre administrateur ou un employé du service d'assistance. Si vous avez créé un utilisateur IAM Identity Center pour votre Compte AWS, une invitation à rejoindre l'utilisateur IAM Identity Center a été envoyée à l'adresse e-mail du. Compte AWS L'URL de connexion spécifique est incluse dans l'invitation par e-mail. Les utilisateurs d'IAM Identity Center ne peuvent pas se connecter via le AWS Management Console. Pour obtenir des instructions détaillées sur la procédure de connexion, voir Se connecter au portail AWS d'accès.

> **Note**
>
> Nous vous recommandons de mettre en signet l'URL de connexion spécifique au portail AWS d'accès afin de pouvoir y accéder rapidement ultérieurement.

Pour plus d'informations sur IAM Identity Center, voir Qu'est-ce qu'IAM Identity Center ?

Identité fédérée

Une identité fédérée est un utilisateur qui peut se connecter à l'aide d'un fournisseur d'identité externe (IdP) connu, tel que Login with Amazon, Facebook, Google ou tout autre IdP compatible avec OpenID Connect (OIDC). Avec la fédération des identités Web, vous pouvez recevoir un jeton d'authentification, puis échanger ce jeton contre des informations d'identification de sécurité temporaires associées à un rôle IAM autorisé à utiliser les ressources de votre Compte AWS. AWS Vous ne vous connectez pas avec le portail AWS Management Console ou n' AWS y accédez pas. C'est plutôt l'identité externe utilisée qui détermine la façon dont vous vous connectez.

Pour plus d'informations, voir Se connecter en tant qu'identité fédérée.

Utilisateur IAM

Un utilisateur IAM est une entité dans AWS laquelle vous créez. Cet utilisateur est une identité au sein de vous Compte AWS qui bénéficie d'autorisations personnalisées spécifiques. Vos informations

d'identification d'utilisateur IAM se composent d'un nom et d'un mot de passe utilisés pour vous connecter au AWS Management Console. Pour obtenir des instructions détaillées sur la procédure de connexion, voir Se connecter en AWS Management Console tant qu'utilisateur IAM.

Pour plus d'informations sur les identités IAM, y compris l'utilisateur IAM, consultez Identités IAM (utilisateurs, groupes d'utilisateurs et rôles).

AWS Utilisateur Builder ID

En tant qu'utilisateur AWS Builder ID, vous vous connectez spécifiquement au AWS service ou à l'outil auquel vous souhaitez accéder. Un utilisateur AWS Builder ID complète ceux Compte AWS que vous possédez déjà ou que vous souhaitez créer. Un AWS Builder ID vous représente en tant que personne, et vous pouvez l'utiliser pour accéder à AWS des services et à des outils sans Compte AWS. Vous disposez également d'un profil dans lequel vous pouvez consulter et mettre à jour vos informations. Pour plus d'informations, voir Se connecter avec le AWS Builder ID.

Prérequis et considérations

Avant de commencer le processus de configuration, examinez les exigences relatives au compte, déterminez si vous en aurez besoin de plusieurs Compte AWS et comprenez les exigences relatives à la configuration de votre compte pour l'accès administratif dans IAM Identity Center.

Compte AWS exigences

Pour vous inscrire à un Compte AWS, vous devez fournir les informations suivantes :

- Un nom de compte — Le nom du compte apparaît à plusieurs endroits, par exemple sur votre facture, et dans des consoles telles que le tableau de bord Billing and Cost Management et la AWS Organizations console.

  Nous vous recommandons d'utiliser une norme de dénomination de compte afin que le nom du compte puisse être facilement reconnu et distingué des autres comptes que vous pourriez posséder. S'il s'agit d'un compte d'entreprise, pensez à utiliser une norme de dénomination telle que organisation - objectif - environnement (par exemple, AnyCompany- audit - prod). S'il s'agit d'un compte personnel, pensez à utiliser une norme de dénomination telle que prénom, nom de famille, objectif (par exemple, paulo-santos-testaccount).
- Une adresse e-mail — Cette adresse e-mail est utilisée comme nom de connexion pour l'utilisateur root du compte et est requise pour le rétablissement du compte, par exemple pour oublier le mot de passe. Vous devez être en mesure de recevoir les messages envoyés à cette adresse e-mail. Avant de pouvoir effectuer certaines tâches, vous devez vérifier que vous avez accès au compte de messagerie.

> **Important**
>
> Si ce compte est destiné à une entreprise, nous vous recommandons d'utiliser une liste de distribution d'entreprise (par exemple,`it.admins@example.com`). Évitez d'utiliser l'adresse e-mail professionnelle d'un individu (par exemple,`paulo.santos@example.com`). Cela permet de garantir que votre entreprise peut accéder au Compte AWS si un employé change de poste ou quitte l'entreprise. L'adresse e-mail peut être utilisée pour réinitialiser les informations d'identification de l'utilisateur root du compte. Assurez-vous de protéger l'accès à cette liste ou adresse de distribution.

- Un numéro de téléphone — Ce numéro peut être utilisé lorsqu'une confirmation de propriété du compte est requise. Vous devez être en mesure de recevoir des appels à ce numéro de téléphone.

> **Important**
>
> Si ce compte est destiné à une entreprise, nous vous recommandons d'utiliser un numéro de téléphone professionnel plutôt qu'un numéro de téléphone personnel. Cela permet de garantir que votre entreprise peut accéder au Compte AWS si un employé change de poste ou quitte l'entreprise.

- Un dispositif d'authentification multifactorielle — Pour sécuriser vos AWS ressources, activez l'authentification multifactorielle (MFA) sur le compte utilisateur root. En plus de vos identifiants de connexion habituels, une authentification secondaire est requise lorsque la MFA est activée, offrant ainsi un niveau de sécurité supplémentaire. Pour plus d'informations sur la MFA, voir Qu'est-ce que la MFA ? dans le guide de l'utilisateur IAM.
- Support plan — Il vous sera demandé de choisir l'un des plans disponibles lors du processus de création de compte. Pour une description des forfaits disponibles, voir Comparer les Support forfaits.

Considérations relatives à l'IAM Identity Center

Les rubriques suivantes fournissent des conseils pour configurer IAM Identity Center pour des environnements spécifiques. Avant de procéder, prenez connaissance des consignes qui s'appliquent à votre environnementPartie 2 : Création d'un utilisateur administratif dans IAM Identity Center.

Rubriques

- Active Directory ou IdP externe
- AWS Organizations
- Rôles IAM
- Pare-feux de nouvelle génération et passerelles Web sécurisées

Active Directory ou IdP externe

Si vous gérez déjà des utilisateurs et des groupes dans Active Directory ou un IdP externe, nous vous recommandons d'envisager de connecter cette source d'identité lorsque vous activez IAM

Identity Center et que vous choisissez votre source d'identité. Cette opération avant de créer des utilisateurs et des groupes dans le répertoire par défaut d'Identity Center vous permettra d'éviter la configuration supplémentaire requise si vous modifiez votre source d'identité ultérieurement.

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

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

  Vous devez disposer d'un AD Connector ou d'un AWS Managed Microsoft AD annuaire AD Connector existant dans votre compte de gestion AWS Directory Service, et celui-ci doit résider dans votre compte AWS Organizations de gestion. Vous ne pouvez connecter qu'un seul AD Connector ou un seul AWS Managed Microsoft AD à la fois. Si vous devez prendre en charge plusieurs domaines ou forêts, utilisez AWS Managed Microsoft AD. Pour plus d'informations, consultez :

  - Connectez un annuaire AWS Managed Microsoft AD à IAM Identity Center dans le guide de l'AWS IAM Identity Center utilisateur.
  - Connectez un annuaire autogéré dans Active Directory à IAM Identity Center dans le guide de l'AWS IAM Identity Center utilisateur.
- Utilisez un Active Directory résidant dans le compte administrateur délégué :

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

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

AWS Organizations

Vous Compte AWS devez être géré par AWS Organizations. Si vous n'avez pas créé d'organisation, vous n'êtes pas obligé de le faire. Lorsque vous activez IAM Identity Center, vous pouvez choisir de AWS créer une organisation pour vous.

Si vous l'avez déjà configuré AWS Organizations, assurez-vous que toutes les fonctionnalités sont activées. Pour de plus amples informations, consultez Activation de toutes les fonctionnalités de l'organisation dans le Guide de l'utilisateur AWS Organizations .

Pour activer IAM Identity Center, vous devez vous connecter au en AWS Management Console utilisant les informations d'identification de votre compte de AWS Organizations gestion. Vous ne pouvez pas activer IAM Identity Center lorsque vous êtes connecté avec les informations d'identification d'un compte AWS Organizations membre. Pour plus d'informations, consultez la section Création et gestion d'une AWS organisation dans le guide de AWS Organizations l'utilisateur.

Rôles IAM

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

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

Pare-feux de nouvelle génération et passerelles Web sécurisées

Si vous filtrez l'accès à des AWS domaines ou points de terminaison d'URL spécifiques à l'aide d'une solution de filtrage de contenu Web telle que NGFWs ou SWGs, vous devez ajouter les domaines ou points de terminaison d'URL suivants aux listes d'autorisation de votre solution de filtrage de contenu Web.

Domaines DNS spécifiques

- *.awsapps.com (http://awsapps.com/)
- *.signin.aws

Points de terminaison d'URL spécifiques

- *[yourdirectory]*https://.awsapps.com/start
- *[yourdirectory]*https://.awsapps.com/login
- https ://*[yourregion]*.signin. aws/platform/login

Utilisation de plusieurs Comptes AWS

Comptes AWS servent de limite de sécurité fondamentale dans AWS. Ils constituent un conteneur de ressources qui fournit un niveau d'isolation utile. La capacité à isoler les ressources et les utilisateurs est essentielle à la mise en place d'un environnement sécurisé et bien gouverné.

La séparation de vos ressources en différentes ressources vous Comptes AWS permet de respecter les principes suivants dans votre environnement cloud :

- Contrôle de sécurité — Les différentes applications peuvent avoir des profils de sécurité différents qui nécessitent des politiques et des mécanismes de contrôle différents. Par exemple, il est plus facile de parler à un auditeur et de trouver un auditeur Compte AWS qui héberge tous les éléments de votre charge de travail soumis aux normes de sécurité du secteur des cartes de paiement (PCI).
- Isolation — An Compte AWS est une unité de protection de sécurité. Les risques potentiels et les menaces de sécurité doivent être maîtrisés à l'intérieur et Compte AWS sans affecter les autres. Les besoins de sécurité peuvent être différents en raison des différentes équipes ou des différents profils de sécurité.
- De nombreuses équipes — Les différentes équipes ont des responsabilités et des besoins en ressources différents. Vous pouvez empêcher les équipes d'interférer les unes avec les autres en les Comptes AWS séparant.
- Isolation des données — En plus d'isoler les équipes, il est important d'isoler les magasins de données d'un compte. Cela peut contribuer à limiter le nombre de personnes pouvant accéder à ce magasin de données et le gérer. Cela permet de limiter l'exposition à des données hautement privées et peut donc contribuer au respect du règlement général sur la protection des données (RGPD) de l'Union européenne.
- Processus métier — Des unités commerciales ou des produits différents peuvent avoir des objectifs et des processus complètement différents. Avec plusieurs Comptes AWS, vous pouvez répondre aux besoins spécifiques d'une unité commerciale.
- Facturation — Un compte est le seul véritable moyen de séparer les éléments au niveau de la facturation. Les comptes multiples permettent de séparer les articles au niveau de la

facturation entre les unités commerciales, les équipes fonctionnelles ou les utilisateurs individuels. Vous pouvez toujours regrouper toutes vos factures auprès d'un seul payeur (en utilisant AWS Organizations et en consolidant la facturation) tout en séparant les articles par Compte AWS.

- Allocation de quotas : les quotas AWS de service sont appliqués séparément pour chacun d'entre eux Compte AWS. La séparation des charges de travail en différentes les Comptes AWS empêche de consommer des quotas les unes pour les autres.

Toutes les recommandations et procédures décrites dans ce guide sont conformes au AWS Well-Architected Framework. Ce cadre est destiné à vous aider à concevoir une infrastructure cloud flexible, résiliente et évolutive. Même si vous commencez modestement, nous vous recommandons de procéder conformément aux directives du cadre. Cela peut vous aider à faire évoluer votre environnement en toute sécurité et sans affecter vos opérations en cours au fur et à mesure de votre croissance.

Avant de commencer à ajouter plusieurs comptes, vous devez élaborer un plan pour les gérer. Pour cela, nous vous recommandons d'utiliser AWS Organizationsun AWS service gratuit pour gérer l'ensemble Comptes AWS de votre organisation.

AWS propose également AWS Control Tower, qui ajoute des couches d'automatisation AWS gérée aux Organizations et l'intègre automatiquement à d'autres AWS services tels qu'Amazon AWS CloudTrail AWS Config CloudWatch AWS Service Catalog, etc. Ces services peuvent entraîner des frais supplémentaires. Pour en savoir plus, consultez Pricing AWS Control Tower (Tarification).

Partie 1 : Configuration d'un nouveau Compte AWS

Ces instructions vous aideront à créer Compte AWS et à sécuriser les informations d'identification de l'utilisateur root. Effectuez toutes les étapes avant de passer àPartie 2 : Création d'un utilisateur administratif dans IAM Identity Center.

Rubriques

- Étape 1 : Ouvrez un AWS compte
- Étape 2 : connectez-vous en tant qu'utilisateur root
- Étape 3 : activer le MFA pour votre utilisateur root Compte AWS

Étape 1 : Ouvrez un AWS compte

1. Ouvrez l'https://portal.aws.amazon.com/billing/inscription.
2. Choisissez Créer un Compte AWS.

   > **Note**
   >
   > Si vous vous êtes connecté AWS récemment, choisissez Se connecter à la console. Si l'option Créer un nouveau compte Compte AWS n'est pas visible, choisissez d'abord Se connecter à un autre compte, puis Créer un nouveau compte Compte AWS.

3. Entrez les informations de votre compte, puis choisissez Continuer.

   Assurez-vous de saisir correctement les informations de votre compte, en particulier votre adresse e-mail. Si vous avez mal saisi votre adresse e-mail, vous ne pouvez pas accéder à votre compte.

4. Choisissez Personnel ou Professionnel.

   La différence entre ces options réside uniquement dans les informations que nous vous demandons. Les deux types de comptes présentent les mêmes caractéristiques et fonctions.

5. Entrez les informations personnelles ou relatives à votre entreprise en vous basant sur les instructions fournies dansCompte AWS exigences.
6. Lisez et acceptez le contrat AWS client.
7. Choisissez Créer un compte et continuer.

À ce stade, vous recevrez un e-mail pour confirmer que votre appareil Compte AWS est prêt à être utilisé. Vous pouvez vous connecter à votre nouveau compte en utilisant l'adresse e-mail et le mot de passe que vous avez fournis lors de votre inscription. Cependant, vous ne pouvez utiliser aucun AWS service tant que vous n'avez pas terminé d'activer votre compte.

8. Sur la page Informations de paiement, saisissez les informations relatives à votre mode de paiement. Si vous souhaitez utiliser une adresse différente de celle que vous avez utilisée pour créer le compte, choisissez Utiliser une nouvelle adresse et entrez l'adresse que vous souhaitez utiliser à des fins de facturation.
9. Choisissez Vérifier et ajouter.

> **Note**
>
> Si votre adresse de contact se trouve en Inde, le contrat d'utilisation de votre compte est conclu avec AISPL, un vendeur AWS local en Inde. Vous devez fournir votre valeur CVV dans le cadre du processus de vérification. Il se peut également que vous deviez saisir un mot de passe à usage unique, selon votre banque. AISPL facture 2 INR à votre mode de paiement dans le cadre du processus de vérification. L'AISPL rembourse les 2 INR une fois la vérification terminée.

10. Pour vérifier votre numéro de téléphone, choisissez le code de votre pays ou de votre région dans la liste et entrez un numéro de téléphone auquel vous pourrez être appelé dans les prochaines minutes. Entrez le code CAPTCHA et soumettez-le.
11. Le système de vérification AWS automatique vous appelle et vous fournit un code PIN. Entrez le code PIN à l'aide de votre téléphone, puis choisissez Continuer.
12. Sélectionnez un Support plan.

    Pour une description des forfaits disponibles, voir Comparer les Support forfaits.

    Une page de confirmation s'affiche pour indiquer que votre compte est en cours d'activation. Cela ne prend généralement que quelques minutes, mais peut parfois prendre jusqu'à 24 heures. Lors de l'activation, vous pouvez vous connecter à votre nouveau Compte AWS. Jusqu'à ce que l'activation soit terminée, vous verrez peut-être un bouton Terminer l'inscription. Vous pouvez l'ignorer.

AWS envoie un e-mail de confirmation lorsque l'activation du compte est terminée. Vérifiez la présence d'un e-mail de confirmation dans votre dossier de courrier électronique et de courrier indésirable. Après avoir reçu ce message, vous avez un accès complet à tous les AWS services.

Étape 2 : connectez-vous en tant qu'utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte.

> **Important**
>
> Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur racine, consultez Tâches nécessitant des informations d'identification d'utilisateur racine dans le Guide de l'utilisateur IAM.

Pour vous connecter en tant qu'utilisateur root

1. Ouvrez le AWS Management Console dossier https://console.aws.amazon.com/.

   > **Note**
   >
   > Si vous vous êtes déjà connecté en tant qu'utilisateur root dans ce navigateur, votre navigateur se souviendra peut-être de l'adresse e-mail du Compte AWS.
   > Si vous vous êtes déjà connecté en tant qu'utilisateur IAM à l'aide de ce navigateur, celui-ci peut afficher la page de connexion de l'utilisateur IAM à la place. Pour revenir à la page de connexion principale, sélectionnez Sign in using root user email (Se connecter à l'aide de l'adresse e-mail de l'utilisateur racine).

2. Si vous ne vous êtes pas déjà connecté à l'aide de ce navigateur, la page principale de connexion s'affiche. Si vous êtes le propriétaire du compte, choisissez Utilisateur root. Entrez l'adresse Compte AWS e-mail associée à votre compte et choisissez Suivant.

3. Vous serez peut-être invité à effectuer un contrôle de sécurité. Effectuez cette opération pour passer à l'étape suivante. Si vous ne parvenez pas à effectuer le contrôle de sécurité, essayez d'écouter le son ou d'actualiser le contrôle de sécurité pour y ajouter un nouveau jeu de caractères.
4. Saisissez votre mot de passe, puis choisissez se connecter.

Étape 3 : activer le MFA pour votre utilisateur root Compte AWS

Pour renforcer la sécurité de vos informations d'identification d'utilisateur root, nous vous recommandons de suivre les meilleures pratiques de sécurité pour activer l'authentification multifactorielle (MFA) pour votre. Compte AWSÉtant donné que l'utilisateur root peut effectuer des opérations sensibles sur votre compte, l'ajout de cette couche d'authentification supplémentaire vous permet de mieux sécuriser votre compte. Il existe plusieurs types de MFA.

Pour obtenir des instructions sur l'activation de l'authentification multifacteur pour l'utilisateur root, consultez la section Activation des appareils MFA pour les utilisateurs du guide de l'utilisateur AWS IAM.

Partie 2 : Création d'un utilisateur administratif dans IAM Identity Center

Une fois que vous avez terminéPartie 1 : Configuration d'un nouveau Compte AWS, les étapes suivantes vous aideront à configurer l' Compte AWS accès d'un utilisateur administratif, qui sera utilisé pour effectuer les tâches quotidiennes.

> **Note**
>
> Cette rubrique décrit les étapes minimales requises pour configurer correctement l'accès administrateur Compte AWS et créer un utilisateur administratif dans IAM Identity Center. Pour plus d'informations, consultez la section Mise en route dans le guide de AWS IAM Identity Center l'utilisateur.

Rubriques

- Étape 1 : activer le centre d'identité IAM
- Étape 2 : Choisissez votre source d'identité
- Étape 3 : Création d'un ensemble d'autorisations administratives
- Étape 4 : configurer Compte AWS l'accès pour un utilisateur administratif
- Étape 5 : Connectez-vous au portail d' AWS accès avec vos informations d'identification administratives

Étape 1 : activer le centre d'identité IAM

> **Note**
>
> Si vous n'avez pas activé l'authentification multifactorielle (MFA) pour votre utilisateur root, Étape 3 : activer le MFA pour votre utilisateur root Compte AWS terminez avant de continuer.

Pour activer IAM Identity Center

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.
2. Ouvrez la console IAM Identity Center.
3. Sous Activer IAM Identity Center, sélectionnez Activer.
4. IAM Identity Center nécessite AWS Organizations. Si vous n'avez pas créé d'organisation, vous devez choisir si vous souhaitez en AWS créer une pour vous. Choisissez Créer une AWS organisation pour terminer ce processus.

   AWS Organizations envoie automatiquement un e-mail de vérification à l'adresse associée à votre compte de gestion. Il peut y avoir un délai avant la réception de l'e-mail de vérification. Validez votre adresse e-mail dans un délai de 24 heures.

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

Étape 2 : Choisissez votre source d'identité

Votre source d'identité dans IAM Identity Center définit l'endroit où vos utilisateurs et vos groupes sont gérés. Vous pouvez choisir l'une des sources d'identité suivantes :

- Répertoire IAM Identity Center : lorsque vous activez IAM Identity Center pour la première fois, il est automatiquement configuré avec un répertoire IAM Identity Center comme source d'identité par défaut. C'est ici que vous créez vos utilisateurs et groupes et que vous attribuez leur niveau d'accès à vos comptes et applications AWS.
- Active Directory : choisissez cette option si vous souhaitez continuer à gérer les utilisateurs dans votre annuaire AWS Managed Microsoft AD à l'aide d'AWS Directory Service ou dans votre annuaire autogéré dans Active Directory (AD).

- Fournisseur d'identité externe : choisissez cette option si vous souhaitez gérer les utilisateurs dans un fournisseur d'identité externe (IdP) tel qu'Okta ou Azure Active Directory.

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

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

Rubriques

- Connectez Active Directory ou un autre IdP et spécifiez un utilisateur
- Utiliser le répertoire par défaut et créer un utilisateur dans IAM Identity Center

Connectez Active Directory ou un autre IdP et spécifiez un utilisateur

Si vous utilisez déjà Active Directory ou un fournisseur d'identité externe (IdP), les rubriques suivantes vous aideront à connecter votre annuaire à IAM Identity Center.

Vous pouvez connecter un AWS Managed Microsoft AD annuaire, un annuaire autogéré dans Active Directory ou un IdP externe à IAM Identity Center. Si vous envisagez de connecter un AWS Managed Microsoft AD annuaire ou un annuaire autogéré dans Active Directory, assurez-vous que votre configuration Active Directory répond aux conditions requises dans. Active Directory ou IdP externe

> **Note**
>
> Pour des raisons de sécurité, nous vous recommandons vivement d'activer l'authentification multifactorielle. Si vous envisagez de connecter un AWS Managed Microsoft AD annuaire ou un annuaire autogéré dans Active Directory et que vous n'utilisez pas RADIUS MFA AWS Directory Service avec, activez l'authentification MFA dans IAM Identity Center. Si vous envisagez d'utiliser un fournisseur d'identité externe, notez que c'est l'IdP externe, et non le IAM Identity Center, qui gère les paramètres MFA. L'authentification MFA dans IAM Identity Center n'est pas prise en charge pour une utilisation par des utilisateurs externes. IdPs Pour plus d'informations, consultez la section Activer le MFA dans le guide de l'AWS IAM Identity Center utilisateur.

AWS Managed Microsoft AD

1. Consultez les instructions de la section Connect to a Microsoft Active Directory.
2. Suivez les étapes décrites dans la section Connecter un annuaire AWS Managed Microsoft AD à IAM Identity Center.
3. Configurez Active Directory pour synchroniser l'utilisateur auquel vous souhaitez accorder des autorisations administratives dans IAM Identity Center. Pour plus d'informations, voir Synchroniser un utilisateur administratif dans IAM Identity Center.

Annuaire autogéré dans Active Directory

1. Consultez les instructions de la section Connect to a Microsoft Active Directory.
2. Suivez les étapes décrites dans la section Connecter un annuaire autogéré dans Active Directory à IAM Identity Center.
3. Configurez Active Directory pour synchroniser l'utilisateur auquel vous souhaitez accorder des autorisations administratives dans IAM Identity Center. Pour plus d'informations, voir Synchroniser un utilisateur administratif dans IAM Identity Center.

IdP externe

1. Consultez les instructions de la section Connect to an external identity provider.
2. Suivez les étapes décrites dans Comment se connecter à un fournisseur d'identité externe.
3.

Configurez votre IdP pour connecter les utilisateurs à IAM Identity Center.

> **Note**
>
> Avant de configurer le provisionnement automatique par groupe de toutes les identités de votre personnel, depuis votre IdP vers IAM Identity Center, nous vous recommandons de synchroniser l'utilisateur auquel vous souhaitez accorder des autorisations administratives dans IAM Identity Center.

Synchroniser un utilisateur administratif dans IAM Identity Center

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

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

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

Étape suivante : Étape 3 : Création d'un ensemble d'autorisations administratives

Utiliser le répertoire par défaut et créer un utilisateur dans IAM Identity Center

Lorsque vous activez IAM Identity Center pour la première fois, il est automatiquement configuré avec un répertoire IAM Identity Center comme source d'identité par défaut. Procédez comme suit pour créer un utilisateur dans IAM Identity Center.

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.
2. Ouvrez la console IAM Identity Center.
3. Suivez les étapes décrites dans Ajouter des utilisateurs pour créer un utilisateur.

   Lorsque vous spécifiez les détails de l'utilisateur, vous pouvez soit envoyer un e-mail contenant les instructions de configuration du mot de passe (il s'agit de l'option par défaut), soit générer un mot de passe à usage unique. Si vous envoyez un e-mail, assurez-vous de spécifier une adresse e-mail à laquelle vous pouvez accéder.
4. Après avoir ajouté l'utilisateur, revenez à cette procédure. Si vous avez conservé l'option par défaut d'envoi d'un e-mail contenant les instructions de configuration du mot de passe, procédez comme suit :

   a. Vous recevrez un e-mail avec pour objet Invitation à rejoindre AWS Single Sign-On. Ouvrez l'e-mail et choisissez Accepter l'invitation.

   b. Sur la page d'inscription d'un nouvel utilisateur, entrez et confirmez un mot de passe, puis choisissez Définir un nouveau mot de passe.

   > **Note**
   >
   > Assurez-vous d'enregistrer votre mot de passe. Vous en aurez besoin plus tardÉtape 5 : Connectez-vous au portail d' AWS accès avec vos informations d'identification administratives.

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

Étape suivante : Étape 3 : Création d'un ensemble d'autorisations administratives

Étape 3 : Création d'un ensemble d'autorisations administratives

Les ensembles d'autorisations sont stockés dans IAM Identity Center et définissent le niveau d'accès des utilisateurs et des groupes à un Compte AWS. Procédez comme suit pour créer un ensemble d'autorisations octroyant des autorisations administratives.

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.
2. Ouvrez la console IAM Identity Center.
3. Dans le volet de navigation d'IAM Identity Center, sous Autorisations multi-comptes, sélectionnez Ensembles d'autorisations.
4. Choisissez Create permission set (Créer un jeu d'autorisations).
5. Pour l'étape 1 : Sélectionnez le type d'ensemble d'autorisations, sur la page Sélectionner le type d'ensemble d'autorisations, conservez les paramètres par défaut et choisissez Suivant. Les paramètres par défaut accordent un accès complet aux AWS services et aux ressources à l'aide de l'ensemble d'autorisations AdministratorAccessprédéfini.

   > **Note**
   >
   > L'ensemble AdministratorAccessd'autorisations prédéfini utilise la politique AdministratorAccess AWS gérée.

6. Pour l'étape 2 : Spécifier les détails de l'ensemble d'autorisations, sur la page Spécifier les détails de l'ensemble d'autorisations, conservez les paramètres par défaut et choisissez Suivant. Le paramètre par défaut limite votre session à une heure.
7. Pour l'étape 3 : révision et création, sur la page Révision et création, procédez comme suit :

   1. Vérifiez le type d'ensemble d'autorisations et confirmez qu'il l'est AdministratorAccess.
   2. Passez en revue la politique AWS gérée et confirmez qu'elle l'est AdministratorAccess.

3. Sélectionnez Create (Créer).

Étape 4 : configurer Compte AWS l'accès pour un utilisateur administratif

Pour configurer Compte AWS l'accès d'un utilisateur administratif dans IAM Identity Center, vous devez attribuer à l'utilisateur le jeu d'AdministratorAccessautorisations.

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.
2. Ouvrez la console IAM Identity Center.
3. Dans le volet de navigation, sous Autorisations multi-comptes, sélectionnez Comptes AWS.
4. Sur la Comptes AWSpage, une liste arborescente de votre organisation apparaît. Cochez la case à côté Compte AWS de laquelle vous souhaitez attribuer un accès administratif. Si votre organisation possède plusieurs comptes, cochez la case à côté du compte de gestion.
5. Choisissez Attribuer des utilisateurs ou des groupes.
6. Pour l'étape 1 : sélectionner les utilisateurs et les groupes, sur la page Attribuer des utilisateurs et des groupes à ***AWS-account-name*** « », procédez comme suit :

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

        Pour filtrer les résultats, commencez à saisir le nom de l'utilisateur souhaité dans le champ de recherche.

    2. Après avoir confirmé que le bon utilisateur est sélectionné, choisissez Next.
7. Pour l'étape 2 : sélectionner des ensembles d'autorisations, sur la page Attribuer des ensembles d'autorisations à ***AWS-account-name*** « », sous Ensembles d'autorisations, sélectionnez l'ensemble AdministratorAccessd'autorisations.
8. Choisissez Suivant.
9. Pour l'étape 3 : Réviser et envoyer, sur la page Réviser et envoyer les devoirs à ***AWS-account-name*** « », procédez comme suit :

    1. Vérifiez l'utilisateur et l'ensemble d'autorisations sélectionnés.

2. Après avoir confirmé que l'ensemble d'AdministratorAccessautorisations est attribué au bon utilisateur, choisissez Soumettre.

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

10. Si l'une des conditions suivantes s'applique, suivez les étapes décrites dans Activer le MFA pour IAM Identity Center :

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

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

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

Étape 5 : Connectez-vous au portail d' AWS accès avec vos informations d'identification administratives

Procédez comme suit pour confirmer que vous pouvez vous connecter au portail AWS d'accès à l'aide des informations d'identification de l'utilisateur administratif et que vous pouvez accéder au Compte AWS.

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.
2. Ouvrez la AWS IAM Identity Center console à l'adresse https://console.aws.amazon.com/singlesignon/.
3. Dans le panneau de navigation, sélectionnez Dashboard (Tableau de bord).
4. Sur la page Tableau de bord, sous Résumé des paramètres, copiez l'URL du portail AWS d'accès.
5. Ouvrez un autre navigateur, collez l'URL du portail AWS d'accès que vous avez copiée et appuyez sur Entrée.
6. Connectez-vous en utilisant l'une des méthodes suivantes :
   - Si vous utilisez Active Directory ou un fournisseur d'identité externe (IdP) comme source d'identité, connectez-vous en utilisant les informations d'identification de l'utilisateur Active Directory ou IdP que vous avez attribué à l'ensemble d'AdministratorAccessautorisations dans IAM Identity Center.
   - Si vous utilisez le répertoire IAM Identity Center par défaut comme source d'identité, connectez-vous en utilisant le nom d'utilisateur que vous avez spécifié lors de la création de l'utilisateur et le nouveau mot de passe que vous avez spécifié pour l'utilisateur.
7. Une fois que vous êtes connecté, une Compte AWSicône apparaît dans le portail.
8. Lorsque vous sélectionnez l'Compte AWSicône, le nom du compte, l'identifiant du compte et l'adresse e-mail associés au compte apparaissent.
9. Choisissez le nom du compte pour afficher l'ensemble d'AdministratorAccessautorisations, puis sélectionnez le lien de la console de gestion situé à droite de AdministratorAccess.

   Lorsque vous vous connectez, le nom de l'ensemble d'autorisations auquel l'utilisateur est attribué apparaît en tant que rôle disponible dans le portail AWS d'accès. Comme vous avez affecté cet utilisateur à l'ensemble d'`AdministratorAccess`autorisations, le rôle apparaîtra dans le portail AWS d'accès sous la forme `AdministratorAccess` :/ *`username`*
10. Si vous êtes redirigé vers la console de AWS gestion, vous avez correctement configuré l'accès administratif au Compte AWS. Passez à l'étape 10.
11. Passez au navigateur que vous avez utilisé pour vous connecter au IAM Identity Center AWS Management Console et le configurer, puis déconnectez-vous de votre utilisateur Compte AWS root.

> **Important**
>
> Nous vous recommandons vivement de suivre les bonnes pratiques consistant à utiliser les informations d'identification de l'utilisateur administratif lorsque vous vous connectez au portail d' AWS accès, et de ne pas utiliser les informations d'identification de l'utilisateur root pour vos tâches quotidiennes.

Pour permettre à d'autres utilisateurs d'accéder à vos comptes et applications, et pour administrer IAM Identity Center, créez et attribuez des ensembles d'autorisations uniquement via IAM Identity Center.

Résolution des problèmes Compte AWS de création

Utilisez les informations fournies ici pour vous aider à résoudre les problèmes liés à la création d'un Compte AWS.

Problèmes

- Je n'ai pas reçu d'appel AWS pour vérifier mon nouveau compte
- Je reçois une erreur concernant le « nombre maximum de tentatives infructueuses » lorsque j'essaie de vérifier mon identité Compte AWS par téléphone
- Cela fait plus de 24 heures et mon compte n'est pas activé

Je n'ai pas reçu d'appel AWS pour vérifier mon nouveau compte

Lorsque vous créez un Compte AWS, vous devez fournir un numéro de téléphone sur lequel vous pouvez recevoir un SMS ou un appel vocal. Vous spécifiez la méthode à utiliser pour vérifier le numéro.

Si vous ne recevez pas le message ou l'appel, vérifiez les points suivants :

- Vous avez saisi le bon numéro de téléphone et sélectionné le bon code de pays lors du processus d'inscription.
- Si vous utilisez un téléphone mobile, assurez-vous de disposer d'un signal cellulaire pour recevoir des SMS ou des appels.
- Les informations que vous avez saisies pour votre mode de paiement sont correctes.

Si vous n'avez pas reçu de SMS ou d'appel pour terminer le processus de vérification d'identité, cela Support peut vous aider à activer votre identité Compte AWS manuellement. Procédez comme suit :

1. Assurez-vous d'être joignable au numéro de téléphone que vous avez fourni pour votre Compte AWS.
2. Ouvrez la AWS Support console, puis choisissez Create case.
   a. Choisissez Support de compte et facturation.
   b. Dans Type, sélectionnez Compte.
   c. Dans Catégorie, sélectionnez Activation.

d. Dans la section Description du cas, indiquez la date et l'heure auxquelles vous pouvez être contacté.
e. Dans la section Options de contact, sélectionnez Chat pour les méthodes de contact.
f. Sélectionnez Envoyer.

> **Note**
>
> Vous pouvez créer un étui Support même si le vôtre Compte AWS n'est pas activé.

Je reçois une erreur concernant le « nombre maximum de tentatives infructueuses » lorsque j'essaie de vérifier mon identité Compte AWS par téléphone

Support peut vous aider à activer manuellement votre compte. Procédez comme suit :

1. Connectez-vous à votre compte en Compte AWS utilisant l'adresse e-mail et le mot de passe que vous avez spécifiés lors de la création de votre compte.
2. Ouvrez la Support console, puis choisissez Create case.
3. Choisissez Account and Billing Support.
4. Dans Type, sélectionnez Compte.
5. Dans Catégorie, sélectionnez Activation.
6. Dans la section Description du cas, indiquez la date et l'heure auxquelles vous pouvez être contacté.
7. Dans la section Options de contact, sélectionnez Chat pour les méthodes de contact.
8. Sélectionnez Envoyer.

Support vous contactera et tentera d'activer manuellement votre Compte AWS.

Cela fait plus de 24 heures et mon compte n'est pas activé

L'activation du compte peut parfois être retardée. Si le processus prend plus de 24 heures, vérifiez les points suivants :

- Terminez le processus d'activation du compte.

  Si vous avez fermé la fenêtre du processus d'inscription avant d'avoir ajouté toutes les informations nécessaires, ouvrez la page d'inscription. Choisissez Se connecter à un compte existant Compte AWS, puis connectez-vous en utilisant l'adresse e-mail et le mot de passe que vous avez choisis pour le compte.
- Vérifiez les informations associées à votre mode de paiement.

  Dans la AWS Billing and Cost Management console, vérifiez la présence d'erreurs dans les modes de paiement.
- Contactez votre institution financière.

  Parfois, les institutions financières rejettent les demandes d'autorisation émanant de AWS. Contactez l'établissement associé à votre mode de paiement et demandez-lui d'approuver les demandes d'autorisation émanant de AWS. AWS annule la demande d'autorisation dès qu'elle est approuvée par votre institution financière, afin que la demande d'autorisation ne vous soit pas facturée. Les demandes d'autorisation peuvent toujours apparaître sous forme de frais minimes (généralement 1 USD) sur les relevés de votre institution financière.
- Vérifiez votre boîte de courrier électronique et votre dossier de courrier indésirable pour toute demande d'informations supplémentaires.
- Essayez un autre navigateur.
- Contacter AWS Support.

  Contactez AWS Supportpour obtenir de l'aide. Mentionnez toutes les étapes de résolution des problèmes que vous avez déjà essayées.

  > **Note**
  >
  > Ne fournissez pas d'informations sensibles, telles que des numéros de carte de crédit, dans toute correspondance avec AWS.

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.