



Guide de l'utilisateur

# AWSConfiguration



# AWSConfiguration: Guide de l'utilisateur

Copyright © 2023 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques et la présentation commerciale d'Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n'est pas d'Amazon, d'une manière susceptible de créer une confusion parmi 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
AWSutilisateurs et informations d'identification .....	5
Utilisateur root .....	5
Utilisateur du centre d'identité IAM .....	6
Identité fédérée .....	6
Utilisateur IAM .....	6
AWSUtilisateur Builder ID .....	7
Prérequis et considérations .....	8
Exigences relatives à Compte AWS .....	8
Considérations relatives à IAM Identity Center .....	9
Active Directory ou IdP externe .....	9
AWS Organizations .....	11
Rôles IAM .....	11
Pare-feux et passerelles Web sécurisées de nouvelle génération .....	11
Utilisation de plusieurs Comptes AWS .....	12
Partie 1 : Configuration d'un nouveauCompte AWS .....	14
Étape 1 : S'inscrire pour un compte AWS .....	14
Étape 2 : connectez-vous en tant qu'utilisateur root .....	16
Pour vous connecter en tant qu'utilisateur root .....	16
Étape 3 : Activez le MFA pour votreCompte AWSutilisateur root .....	17
Partie 2 : Création d'un utilisateur administratif dans IAM Identity Center .....	18
Étape 1 : activer IAM Identity Center .....	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 : ConfigurationCompte AWSaccès pour un utilisateur administratif .....	25
Étape 5 : Connectez-vous auAWSaccédez au portail avec vos informations d'identification administratives .....	26
Résolution des problèmesCompte AWSproblèmes de création .....	29
Je n'ai pas reçu l'appel deAWSpour vérifier mon nouveau compte .....	29
Je reçois un message d'erreur concernant le « nombre maximum de tentatives infructueuses » lorsque j'essaie de vérifier monCompte AWSpar téléphone .....	30
Cela fait plus de 24 heures et mon compte n'est pas activé .....	31
.....	xxxii

# Présentation

Ce guide fournit des instructions pour créer un nouveau Compte AWS et configurer votre premier utilisateur administratif dans AWS IAM Identity Center en suivant les meilleures pratiques de sécurité les plus récentes.

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

- **Réceptacle**— Un Compte AWS est un conteneur pour tous 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 (Amazon EC2) 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 du compte qui contient ou possède la ressource.
- **Limite de sécurité**— Un Compte AWS est la limite de sécurité de base de votre AWS ressources. Les ressources que vous créez dans votre compte ne sont disponibles que pour les utilisateurs disposant d'informations d'identification pour ce même compte.

Parmi les ressources clés que vous pouvez créer dans votre compte figurent des identités, tels 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, du répertoire IAM Identity Center ou de tout autre utilisateur accédant Services AWS en utilisant les informations d'identification fournies par le biais d'une source d'identité. Ces identités comportent des informations d'identification que quelqu'un peut utiliser pour se connecter, ou authentifier pour AWS. Les identités sont également associées à 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.

## Profile

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 [AWSBuilder 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 utilisateurCompte 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.



# AWSUtilisateurs et informations d'identification

Lorsque vous interagissez avecAWS, vous spécifiez vos informations de AWS sécurité pour vérifier qui vous êtes et si vous êtes autorisé à accéder aux ressources que vous demandez. AWSutilise 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 votreCompte 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 celle de l'utilisateur root du AWS compte. Vous pouvez vous connecter en [AWS Management Console](#) tant 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 avec une seule identité de connexion disposant d'un accès complet à tous les Services AWS et ressources du compte. Cette identité est appelée utilisateur root du Compte AWS. Vous pouvez y accéder en vous connectant à l'aide de l'adresse électronique et du mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur root pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur root et utilisez-les pour effectuer les tâches que seul l'utilisateur root peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur root, veuillez consulter [Tâches nécessitant les informations d'identification de l'utilisateur root](#) 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 leAWS 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'AWSy 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 \(utilisateurs, groupes d'utilisateurs et rôles\)](#).

## AWSUtilisateur 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 sansCompte 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, passez en revue les exigences relatives au compte et déterminez si vous en aurez besoin de plusieurs Comptes AWS, et comprenez les exigences relatives à la configuration de votre compte pour un accès administratif dans IAM Identity Center.

## Exigences relatives à Compte AWS

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 de facturation et de gestion des coûts et le 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 détenir. 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 récupérer le 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'une personne (par exemple, `paulo.santos@example.com`). Cela permet à votre entreprise d'accéder au Compte AWS si un salarié 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 de distribution ou à cette adresse.

- Un numéro de téléphone— Ce numéro peut être utilisé lorsque la confirmation de la 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 à votre entreprise d'accéder au Compte AWS si un salarié change de poste ou quitte l'entreprise.

- Un dispositif d'authentification multifactoriel— 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 l'authentification MFA est activée, fournissant ainsi un niveau de sécurité supplémentaire. Pour plus d'informations sur l'authentification multifactorielle, voir [Qu'est-ce que le MFA ?](#) dans le Guide de l'utilisateur IAM.
- AWS Supportplan— Il vous sera demandé de choisir l'un des plans disponibles lors du processus de création du compte. Pour une description des plans disponibles, voir [Comparez AWS Supportplans](#).

## Considérations relatives à IAM Identity Center

Les rubriques suivantes fournissent des conseils pour configurer IAM Identity Center pour des environnements spécifiques. Comprenez les instructions qui s'appliquent à votre environnement avant de passer à [Partie 2 : Création d'un utilisateur administratif dans IAM Identity Center](#).

### Rubriques

- [Active Directory ou IdP externe](#)
- [AWS Organizations](#)
- [Rôles IAM](#)
- [Pare-feux et passerelles Web sécurisées de nouvelle génération](#)

## Active Directory ou IdP externe

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

IAM Identity Center et que vous choisissiez votre source d'identité. En procédant ainsi avant de créer des utilisateurs et des groupes dans le répertoire par défaut d'Identity Center, vous éviterez la configuration supplémentaire requise si vous modifiez ultérieurement votre source d'identité.

Si vous souhaitez utiliser Active Directory comme source d'identité, votre configuration doit répondre aux prérequis suivants :

- Si vous utilisez AWS Managed Microsoft AD, vous devez activer IAM Identity Center dans la même Région AWS où votre AWS Managed Microsoft AD répertoire 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 basculer vers la région dans laquelle IAM Identity Center est configuré. Notez également que le portail 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 connecteur AD existant ou AWS Managed Microsoft AD répertoire configuré dans AWS Directory Service, et il doit se trouver dans votre AWS Organizations compte de gestion. Vous ne pouvez connecter qu'un seul connecteur AD ou un 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, reportez-vous à :

- [Connecter un répertoire dans AWS Managed Microsoft AD vers IAM Identity Center](#) dans le AWS IAM Identity Center Guide de l'utilisateur.
- [Connecter un répertoire autogéré dans Active Directory à IAM Identity Center](#) dans le AWS IAM Identity Center Guide de l'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 connecteur AD existant ou AWS Managed Microsoft AD répertoire configuré dans AWS répertoire résidant dans le compte administrateur délégué.

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

## AWS Organizations

Votre Compte AWS doit 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 d'avoir AWS créer une organisation pour vous.

Si vous 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 AWS Management Console en utilisant les informations d'identification de votre AWS Organizations compte de gestion. Vous ne pouvez pas activer IAM Identity Center lorsque vous êtes connecté à l'aide des informations d'identification d'un AWS Organizations compte membre. Pour plus d'informations, voir [Création et gestion d'un AWS Organisation](#) dans le AWS Organizations Guide de l'utilisateur.

## Rôles IAM

Si vous avez déjà configuré des rôles IAM dans votre Compte AWS, nous vous recommandons de vérifier si votre compte approche du quota pour les rôles IAM. Pour plus d'informations, voir [Quotas d'objets IAM](#).

Si vous approchez du quota, pensez à demander une augmentation de quota. Dans le cas contraire, 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 des quotas de service.

## Pare-feux et passerelles Web sécurisées de nouvelle génération

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

### Domaines DNS spécifiques

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

## Points de terminaison d'URL spécifiques

- [https ://\[votre répertoire\].awsapps.com/start](https://[votre répertoire].awsapps.com/start)
- [https ://\[votre répertoire\].awsapps.com/login](https://[votre répertoire].awsapps.com/login)
- [https ://\[votre région\].signin.aws/platform/login](https ://[votre région].signin.aws/platform/login)

## Utilisation de plusieurs Comptes AWS

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

Séparer vos ressources en plusieurs Comptes AWS vous aide à appliquer les principes suivants dans votre environnement cloud :

- **Contrôle de sécurité**— 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 d'être en mesure de pointer du doigt un seul auditeur Compte AWS qui héberge tous les éléments de votre charge de travail soumis à [Normes de sécurité du secteur des cartes de paiement \(PCI\)](#).
- **Isolement**— Un Compte AWS est une unité de protection de sécurité. Les risques potentiels et les menaces de sécurité doivent être contenus dans un Compte AWS sans affecter les autres. Les besoins en matière 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 séparant Comptes AWS.
- **Isolation des données**— En plus d'isoler les équipes, il est important d'isoler les magasins de données par rapport à un compte. Cela peut aider 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 à la conformité avec [la 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 éléments 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 facturation consolidée) tout en séparant les rubriques par [Compte AWS](#).
- **Allocation de quotas**— [AWS](#) les quotas de service sont appliqués séparément pour chacun [Compte AWS](#). Séparer les charges de travail en différentes [Comptes AWS](#) les empêche de consommer des quotas les uns pour les autres.

Toutes les recommandations et procédures décrites dans ce guide sont conformes à la [AWS Un cadre bien structuré](#). Ce framework est destiné à vous aider à concevoir une infrastructure cloud flexible, résiliente et évolutive. Même si vous commencez modestement, nous vous recommandons de suivre les instructions 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 Organizations](#), qui est gratuit [AWS](#) service, pour gérer tous les [Comptes AWS](#) dans votre organisation.

[AWS](#) propose également [AWS Control Tower](#), qui ajoute des couches de [AWS](#) gestion de l'automatisation aux organisations et l'intègre automatiquement à d'autres [AWS](#) services tels que [AWS CloudTrail](#), [AWS Config](#), [Amazon CloudWatch](#), [AWS Service Catalog](#), et d'autres. Ces services peuvent entraîner des coûts 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 un Compte AWS et sécurisez les informations d'identification de l'utilisateur root. Effectuez toutes les étapes avant de passer à [Partie 2 : Création d'un utilisateur administratif dans IAM Identity Center](#).

## Rubriques

- [Étape 1 : S'inscrire pour un compte AWS](#)
- [Étape 2 : connectez-vous en tant qu'utilisateur root](#)
- [Étape 3 : Activez le MFA pour votre Compte AWS utilisateur root](#)

## Étape 1 : S'inscrire pour un compte AWS

1. Ouvrez <https://portal.aws.amazon.com/billing/signup>.
2. Choisissez **Créer un Compte AWS**.

### Note

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

3. Entrez les informations de votre compte, puis choisissez **Poursuivre**.

Assurez-vous de saisir correctement les informations de votre compte, en particulier votre adresse e-mail. Si vous saisissez une adresse e-mail incorrecte, vous ne pourrez 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 relatives à votre entreprise ou à votre personne en suivant les instructions fournies dans [Exigences relatives à Compte AWS](#).
6. Lisez et acceptez le [AWS Contrat avec le client](#).
7. Choisissez **Créer un compte et continuer**.

À ce stade, vous recevrez un e-mail confirmant que votre 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 pas en utiliser AWS services jusqu'à ce que vous ayez fini d'activer votre compte.

8. Sur la page Informations de paiement, entrez 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, votre contrat d'utilisation pour votre compte est conclu avec AISPL, une société locale AWS vendeur 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. L'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 saisissez un numéro de téléphone auquel vous pourrez être appelé dans les prochaines minutes. Entrez le code CAPTCHA, puis validez.
11. Le AWS un système de vérification automatique vous appelle et vous fournit un code PIN. Entrez le code PIN à l'aide de votre téléphone, puis choisissez Poursuivre.
12. Sélectionnez un AWS Support plan.

Pour une description des plans disponibles, voir [Comparez AWS Support plans](#).

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. Pendant l'activation, vous pouvez vous connecter à votre nouveau Compte AWS. Jusqu'à ce que l'activation soit terminée, vous pouvez voir un bouton Inscription complète. Vous pouvez l'ignorer.

AWS envoie un e-mail de confirmation lorsque l'activation du compte est terminée. Vérifiez la présence du message électronique de confirmation dans vos e-mails et dans votre

dossier de courrier indésirable. Après avoir reçu ce message, vous avez un accès complet à tousAWSservices.

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

Lorsque vous créez un Compte AWS pour la première fois, vous commencez avec une seule identité de connexion disposant d'un accès complet à tous les Services AWS et ressources du compte. Cette identité est appelée utilisateur root du Compte AWS. Vous pouvez y accéder en vous connectant à l'aide de l'adresse électronique et du mot de passe que vous avez utilisés pour créer le compte.

### Important

Il est vivement recommandé de ne pas utiliser l'utilisateur root pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur root et utilisez-les pour effectuer les tâches que seul l'utilisateur root peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur root, veuillez consulter [Tâches nécessitant les informations d'identification de l'utilisateur root](#) dans le Guide de l'utilisateur IAM.

## Pour vous connecter en tant qu'utilisateur root

1. Ouvrez la console AWS Management Console à l'adresse <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 Root user. Entrez l'adresse Compte AWS e-mail associée à votre compte et choisissez Suivant.

3. Il se peut que vous soyez 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 : Activez le MFA pour votre Compte AWS Utilisateur root

Pour améliorer 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 AWS. Étant donné que l'utilisateur root peut effectuer des opérations sensibles sur votre compte, l'ajout de ce niveau d'authentification supplémentaire vous permet de mieux sécuriser votre compte. Il existe plusieurs types de MFA.

Pour obtenir des instructions sur l'activation de la MFA pour l'utilisateur root, voir [Activation des appareils MFA pour les utilisateurs dans AWS](#) dans le Guide de l'utilisateur IAM.

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

Une fois que vous avez terminé [Partie 1 : Configuration d'un nouveau Compte AWS](#), les étapes suivantes vous aideront à configurer l'accès pour un utilisateur administratif, qui sera utilisé pour effectuer des tâches quotidiennes.

### Note

Cette rubrique décrit les étapes minimales requises pour configurer correctement l'accès administrateur pour un [Compte AWS](#) et créer un utilisateur administratif dans IAM Identity Center. Pour plus d'informations, voir [Pour démarrer](#) dans le [AWS IAM Identity Center Guide de l'utilisateur](#).

### Rubriques

- [Étape 1 : activer IAM Identity Center](#)
- [Étape 2 : Choisissez votre source d'identité](#)
- [Étape 3 : Création d'un ensemble d'autorisations administratives](#)
- [Étape 4 : Configuration de l'accès pour un utilisateur administratif](#)
- [Étape 5 : Connectez-vous au portail avec vos informations d'identification administratives](#)

## Étape 1 : activer IAM Identity Center

### Note

Si vous n'avez pas activé l'authentification multifactorielle (MFA) pour votre utilisateur root, complétez [Étape 3 : Activez le MFA pour votre utilisateur root](#) avant de poursuivre.

## Pour activer IAM Identity Center

1. Connectez-vous à la [AWS Management Console](#) en tant que propriétaire du compte en sélectionnant Root user (Utilisateur racine) et en saisissant l'adresse e-mail de Compte AWS. Sur la page suivante, saisissez votre mot de passe.
2. Ouvrez le [Console IAM Identity Center](#).
3. Sous Activer IAM Identity Center, choisissez Activer.
4. IAM Identity Center nécessite AWS Organizations. Si vous n'avez pas encore créé d'organisation, vous devez choisir d'avoir AWS. Créez-en un pour vous. Choisissez Créez 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. Avec 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, voir [Administration déléguée](#) dans le AWS IAM Identity Center Guide de 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 vos 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 qui ont 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 sur votre Compte AWS.

### Important

Si vous gérez déjà des utilisateurs et des groupes dans Active Directory ou auprès d'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 attributions. Si vous gérez déjà des utilisateurs et des groupes dans une source d'identité, le fait de passer à une autre source d'identité peut entraîner la suppression de 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 leur Comptes AWS et 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 un répertoire, un annuaire autogéré dans Active Directory ou un IdP externe avec IAM Identity Center. Si vous envisagez de connecter un AWS Managed Microsoft AD répertoire ou 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 répertoire ou répertoire autogéré dans Active Directory et vous n'utilisez pas RADIUS MFA avec AWS Directory Service, activez l'authentification multifactorielle dans IAM Identity Center. Si vous envisagez d'utiliser un fournisseur d'identité externe, notez que c'est l'IdP externe, et non IAM Identity Center, qui gère les paramètres MFA. L'authentification multifactorielle dans IAM Identity Center n'est pas prise en charge pour une utilisation par des IdPs. Pour plus d'informations, voir [Activer le MFA](#) dans le AWS IAM Identity Center Guide de l'utilisateur.

### AWS Managed Microsoft AD


1. Consultez les directives figurant dans [Se connecter à un Microsoft Active Directory](#).
2. Suivez les étapes décrites dans [Connecter un répertoire dans AWS Managed Microsoft AD vers 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](#).

### Répertoire autogéré dans Active Directory

1. Consultez les directives figurant dans [Se connecter à un Microsoft Active Directory](#).
2. Suivez les étapes décrites dans [Connecter un répertoire 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 directives figurant dans [Connectez-vous à un fournisseur d'identité externe](#).
2. Suivez les étapes décrites dans [Comment se connecter à un fournisseur d'identité externe](#).
3. Configurez votre IdP pour provisionner des utilisateurs dans IAM Identity Center.

 Note

Avant de configurer le provisionnement automatique par groupe de toutes les identités de vos collaborateurs 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 dans IAM Identity Center.

1. Ouvrez le [Console IAM Identity Center](#).
2. Sélectionnez Settings (Paramètres).
3. Sur le Réglages page, choisissez Source d'identité onglet, choisissez Actions, puis choisissez Gérer la synchronisation.
4. Sur le Gérer la synchronisation page, choisissez Utilisateurs onglet, puis choisissez Ajouter des utilisateurs et des groupes.
5. Sur le Utilisateurs onglet, 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 Submit (Envoyer).
7. Dans le Gérer la synchronisation page, l'utilisateur que vous avez spécifié apparaît dans Utilisateurs dans le périmètre de synchronisation liste.
8. Dans le panneau de navigation, choisissez utilisateurs.
9. Sur le 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 à la [AWS Management Console](#) en tant que propriétaire du compte en sélectionnant Root user (Utilisateur racine) et en saisissant l'adresse e-mail de Compte AWS. Sur la page suivante, saisissez votre mot de passe.
2. Ouvrez le [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'envoyer un e-mail avec les instructions de configuration du mot de passe, procédez comme suit :
  - a. Vous recevrez un e-mail avec l'objet Invitation à adhérer AWSAuthentification unique. Ouvrez l'e-mail et choisissez Accepter l'invitation.
  - b. Sur le Inscription d'un nouvel utilisateur page, 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 tard pour [Étape 5 : Connectez-vous au AWS accédez au portail 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 Compte AWS. Procédez comme suit pour créer un ensemble d'autorisations qui octroie des autorisations administratives.

1. Connectez-vous à la [AWS Management Console](#) en tant que propriétaire du compte en sélectionnant Root user (Utilisateur racine) et en saisissant l'adresse e-mail de Compte AWS. Sur la page suivante, saisissez votre mot de passe.
2. Ouvrez le [Console IAM Identity Center](#).
3. Dans le volet de navigation d'IAM Identity Center, sous Autorisations multi-comptes, choisissez Ensembles d'autorisations.
4. Choisissez Create permission set (Créer un jeu d'autorisations).
5. Pour Étape 1 : Sélectionnez le type d'ensemble d'autorisations, sur le Sélectionnez le type d'ensemble d'autorisations page, conservez les paramètres par défaut et choisissez Suivant. Les paramètres par défaut accordent un accès complet à AWS services et ressources utilisant AdministratorAccess ensemble d'autorisations prédéfini.

### Note

Le prédéfini AdministratorAccess le jeu d'autorisations utilise AdministratorAccess AWS politique gérée.

6. Pour Étape 2 : Spécifier les détails de l'ensemble d'autorisations, sur le Spécifier les détails de l'ensemble d'autorisations page, conservez les paramètres par défaut et choisissez Suivant. Le paramètre par défaut limite votre session à une heure.
7. Pour Étape 3 : Révision et création, sur le Révision et création page, procédez comme suit :
  1. Vérifiez le type d'ensemble d'autorisations et confirmez qu'il est AdministratorAccess.
  2. Passez en revue le AWS politique gérée et confirmez qu'elle l'est AdministratorAccess.

3. Sélectionnez Create (Créer).


## Étape 4 : Configuration Compte AWS accès pour un utilisateur administratif

Pour configurer Compte AWS accès pour un utilisateur administratif dans IAM Identity Center, vous devez attribuer à l'utilisateur AdministratorAccess ensemble d'autorisations.

1. Connectez-vous à la [AWS Management Console](#) en tant que propriétaire du compte en sélectionnant Root user (Utilisateur racine) et en saisissant l'adresse e-mail de Compte AWS. Sur la page suivante, saisissez votre mot de passe.
2. Ouvrez le [Console IAM Identity Center](#).
3. Dans le volet de navigation, sous Autorisations multi-comptes, choisissez Comptes AWS.
4. Sur le Comptes AWS, une liste arborescente de votre organisation s'affiche. Cochez la case située à côté du Compte AWS auquel 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 Étape 1 : Sélection des utilisateurs et des groupes, sur le Attribuez des utilisateurs et des groupes à »**AWS-nom-compte**« page, procédez comme suit :
  1. Sur le Utilisateurs onglet, sélectionnez l'utilisateur auquel vous souhaitez accorder des autorisations administratives.

Pour filtrer les résultats, commencez à saisir le nom de l'utilisateur que vous souhaitez dans le champ de recherche.
  2. Après avoir confirmé que le bon utilisateur est sélectionné, choisissez Suivant.
7. Pour Étape 2 : Sélection des ensembles d'autorisations, sur le Attribuer des ensembles d'autorisations à »**AWS-nom-compte**« page, sous Ensembles d'autorisations, sélectionnez le AdministratorAccess ensemble d'autorisations.
8. Choisissez Suivant.
9. Pour Étape 3 : Révision et soumission, sur le Vérifiez et soumettez les devoirs à »**AWS-nom-compte**« page, procédez comme suit :
  1. Vérifiez l'utilisateur et l'ensemble d'autorisations sélectionnés.


- Après avoir vérifié que le bon utilisateur est affecté au `AdministratorAccess` ensemble d'autorisations, 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.

- Si l'une des situations suivantes s'applique, suivez les étapes décrites dans [Activer le MFA](#) pour activer la MFA pour IAM Identity Center :

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

 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 multifactorielle 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 `Compte AWS`, et les politiques spécifiées dans l'ensemble d'autorisations sont associées au rôle.

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

Procédez comme suit pour confirmer que vous pouvez vous connecter au `AWS` accédez au portail en utilisant les informations d'identification de l'utilisateur administratif et que vous pouvez accéder au `Compte AWS`.

1. Connectez-vous à la [AWS Management Console](#) en tant que propriétaire du compte en sélectionnant Root user (Utilisateur racine) et en saisissant l'adresse e-mail de Compte AWS. Sur la page suivante, saisissez votre mot de passe.
  2. Ouvrez leAWS IAM Identity Centerconsole à<https://console.aws.amazon.com/singlesignon/>.
  3. Dans le panneau de navigation, sélectionnez Dashboard (Tableau de bord).
  4. Sur leTableau de bordpage, sousRésumé des paramètres, copiez leAWSURL du portail d'accès.
  5. Ouvrez un autre navigateur, collez leAWSs'accédez à l'URL du portail que vous avez copiée et appuyez surEntrez.
  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 à l'aide des informations d'identification de l'utilisateur Active Directory ou IdP que vous avez attribué auAdministratorAccessautorisation définie 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, unCompte AWSl'icône apparaît dans le portail.
  8. Lorsque vous sélectionnez leCompte 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 leAdministratorAccessensemble d'autorisations, puis sélectionnez leConsole de gestionlien à droite deAdministratorAccess.
- Lorsque vous vous connectez, le nom de l'ensemble d'autorisations auquel l'utilisateur est affecté apparaît en tant que rôle disponible dans leAWSportail d'accès. Parce que vous avez assigné cet utilisateur auAdministratorAccessensemble d'autorisations, le rôle apparaîtra dansAWSs'accéder au portail en tant que :AdministratorAccess/*nom d'utilisateur*
10. Si vous êtes redirigé versAWSConsole de gestion, vous avez correctement configuré l'accès administratif àCompte AWS. Passez à l'étape 10.
  11. Accédez au navigateur que vous avez utilisé pour vous connecter auAWS Management Consoleet configurez IAM Identity Center, puis déconnectez-vous de votreCompte AWSutilisateur root.

**⚠ Important**

Nous vous recommandons vivement de respecter les meilleures pratiques qui consistent à utiliser les informations d'identification de l'utilisateur administratif lorsque vous vous connectez auAWSportail d'accès, et que vous n'utilisiez pas 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 de création de compte AWS

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 l'appel de AWS pour vérifier mon nouveau compte](#)
- [Je reçois un message d'erreur concernant le « nombre maximum de tentatives infructueuses » lorsque j'essaie de vérifier mon compte AWS par téléphone](#)
- [Cela fait plus de 24 heures et mon compte n'est pas activé](#)

## Je n'ai pas reçu l'appel de 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 portable, 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, AWS Support peut vous aider à activer votre 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 le [AWS Support console](#), puis choisissez Créer un dossier.
  - a. Choisissez Support de compte et facturation.
  - b. Pour Type, sélectionnez Compte.

- c. Pour **Catégorie**, sélectionnez **Activation**.
- d. Dans le **Description du cas** section, indiquez la date et l'heure auxquelles vous pouvez être contacté.
- e. Dans le **Options de contact** section, sélectionnez **Discuter** pour **Méthodes de contact**.
- f. Sélectionnez **Submit (Envoyer)**.

 **Note**

Vous pouvez créer un dossier avec **AWS Support** même si votre **Compte AWS** n'est pas activé.

## Je reçois un message d'erreur concernant le « nombre maximum de tentatives infructueuses » lorsque j'essaie de vérifier mon **Compte AWS** par téléphone

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

1. [Connectez-vous à votre \*\*Compte AWS\*\*](#) en utilisant l'adresse e-mail et le mot de passe que vous avez spécifiés lors de la création de votre compte.
2. Ouvrez le [AWS Support console](#), puis choisissez **Créer un dossier**.
3. Choisissez **Assistance relative aux comptes et à la facturation**.
4. Pour **Type**, sélectionnez **Compte**.
5. Pour **Catégorie**, sélectionnez **Activation**.
6. Dans le **Description du cas** section, indiquez la date et l'heure auxquelles vous pouvez être contacté.
7. Dans le **Options de contact** section, sélectionnez **Discuter** pour **Méthodes de contact**.
8. Sélectionnez **Submit (Envoyer)**.

**AWS 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'ajouter toutes les informations nécessaires, ouvrez le [enregistrement](#) page. Choisissez [Connectez-vous à un compte existant](#) Compte AWS, puis connectez-vous à l'aide de l'adresse e-mail et du mot de passe que vous avez choisis pour le compte.

- Vérifiez les informations associées à votre mode de paiement.

Dans le [AWS Billing and Cost Management](#) console, vérifiez [Modes de paiement](#) pour les erreurs.

- 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, de sorte que la demande d'autorisation ne vous est 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 vos e-mails et votre dossier de courrier indésirable pour les demandes d'informations supplémentaires.
- Essayez un autre navigateur.
- Contacter [AWS Support](#).

Contactez [AWS Support](#) pour obtenir de l'aide. Mentionnez toutes les étapes de dépannage 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.