Guide de l’utilisateur

AWS Configuration

AWS Configuration: Guide de l’utilisateur

Table of Contents

Présentation

Ce guide fournit des instructions pour créer un nouveauCompte AWSet configurez votre premier utilisateur administratif dansAWS IAM Identity Centeren suivant les meilleures pratiques de sécurité les plus récentes.

UnCompte AWSest nécessaire pour accéderServices AWSet remplit deux fonctions de base :

- Récipient— UnCompte AWSest un conteneur pour tous lesAWSressources que vous pouvez créer en tant queAWSclient. 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 unressourcedans 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— UnCompte AWSest la limite de sécurité de base de votreAWSressources. 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 figurentidentités, 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 accédantServices AWSen 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, ouauthentifierpourAWS. 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 IAM administrateur. 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'autorisation supérieur pour Compte AWS par rapport aux autres membres de leur organisation. Les administrateurs établissent et mettent en œuvre des paramètres pour Compte AWS. Ils créent également des utilisateurs IAM d'IAMIdentity Center. L'administrateur fournit à ces utilisateurs leurs informations d'accès et un identifiant URL pour se connecter à AWS.

Compte

Une norme Compte AWS contient à la fois votre AWS les 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 à AWS pour vous connecter et accéder à 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 (MFA) à usage unique. 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. Entrée 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 votre 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 AWS pour être 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 à 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 Compte AWS, voir AWS Builder ID et autres AWS informations d'identification.

Utilisateur

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

Informations d'identification de l'utilisateur root

Les informations d'identification de l'utilisateur root sont les mêmes que celles utilisées pour se connecter à AWS Management Console en tant qu'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 votre AWS des identifiants de 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 AWS services et ressources dans votre Compte AWS. Lorsque vous créez pour la première fois un Compte AWS, vous commencez avec une identité de connexion unique offrant un accès complet à tous AWS services et ressources du compte. Cette identité est AWS utilisateur root du compte. Vous pouvez vous connecter au AWS Management Consoleen tant qu'utilisateur root en utilisant l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Pour obtenir des instructions détaillées sur la procédure de connexion, voir Se connecter au AWS Management Console en tant qu'utilisateur root.

> **Important**
>
> Lorsque vous créez un Compte AWS, vous commencez avec une seule identité de connexion qui donne un accès complet à tous Services AWS et les ressources du compte. Cette identité s'appelle Compte AWS utilisateur 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 nécessitent que vous vous connectiez en tant qu'utilisateur root, consultez la section Tâches nécessitant des informations d'identification utilisateur root dans le Guide de IAM l'utilisateur.

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

IAMUtilisateur du centre d'identité

Un utilisateur IAM d'Identity Center se connecte via le AWS portail d'accès. Le AWS un portail d'accès ou une connexion spécifique URL 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 IAM l'utilisateur Identity Center a été envoyée à l'adresse e-mail du Compte AWS. La connexion spécifique URL est incluse dans l'invitation par e-mail. IAMLes utilisateurs d'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 AWS portail d'accès.

> **Note**
>
> Nous vous recommandons d'ajouter la connexion URL spécifique à vos favoris pour AWS portail d'accès afin que vous puissiez y accéder rapidement ultérieurement.

Pour plus d'informations sur IAM Identity Center, consultez Qu'est-ce qu'IAMIdentity 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 dans AWS qui correspondent à un IAM rôle autorisé à utiliser les ressources de votre Compte AWS. Vous ne vous connectez pas avec le AWS Management Console or AWS portail d'accès. L'identité externe utilisée détermine plutôt la manière dont vous vous connectez.

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

IAMutilisateur

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

IAM d'identification d'utilisateur 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 au AWS Management Console en tant qu'IAMutilisateur.

Pour plus d'informations sur les IAM identités, y compris l'IAMutilisateur, voir IAMIdentités (utilisateurs, groupes d'utilisateurs et rôles).

AWS Utilisateur Builder ID

En tant que AWS Utilisateur Builder ID, vous vous connectez spécifiquement au AWS service ou outil auquel vous souhaitez accéder. Un AWS L'utilisateur Builder ID complète tout Compte AWS vous possédez déjà ou souhaitez créer. Un AWS Le Builder ID vous représente en tant que personne et vous pouvez l'utiliser pour accéder AWS services et outils sans Compte AWS. Vous avez également un profil dans lequel vous pouvez consulter et mettre à jour vos informations. Pour plus d'informations, voir Pour se connecter avec AWS ID du constructeur.

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 plusieursCompte 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 àCompte 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 leAWS Organizationsconsole.

  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 queorganisation-objectif-environnement(par exemple,AnyCompany-audit-prod). S'il s'agit d'un compte personnel, pensez à utiliser une norme de dénomination telle queprénom-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 auCompte AWSsi 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 auCompte AWSsi un salarié change de poste ou quitte l'entreprise.

- Un dispositif d'authentification multifactoriel— Pour sécuriser votreAWSressources, 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, voirQu'est-ce que le MFA ?dans leGuide 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, voirComparezAWS 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 àPartie 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 choisissez 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 utilisezAWS Managed Microsoft AD, vous devez activer IAM Identity Center dans le mêmeRégion AWSoù votreAWS Managed Microsoft ADle 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 leAWSle 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 ouAWS Managed Microsoft ADrépertoire configuré dansAWS Directory Service, et il doit se trouver dans votreAWS Organizationscompte de gestion. Vous ne pouvez connecter qu'un seul connecteur AD ou unAWS Managed Microsoft ADà la fois. Si vous devez prendre en charge plusieurs domaines ou forêts, utilisezAWS Managed Microsoft AD. Pour plus d'informations, reportez-vous à :

  - Connecter un répertoire dansAWS Managed Microsoft ADvers IAM Identity Centerdans leAWS IAM Identity CenterGuide de l'utilisateur.
  - Connecter un répertoire autogéré dans Active Directory à IAM Identity Centerdans leAWS IAM Identity CenterGuide 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 ouAWS Managed Microsoft ADrépertoire configuré dansAWSrépertoire 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

VotreCompte AWSdoit être géré parAWS 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'avoirAWScréez une organisation pour vous.

Si vous avez déjà configuréAWS 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 auAWS Management Consoleen utilisant les informations d'identification de votreAWS Organizationscompte de gestion. Vous ne pouvez pas activer IAM Identity Center lorsque vous êtes connecté à l'aide des informations d'identification d'unAWS Organizationscompte membre. Pour plus d'informations, voirCréation et gestion d'unAWSOrganisationdans leAWS OrganizationsGuide de l'utilisateur.

Rôles IAM

Si vous avez déjà configuré des rôles IAM dans votreCompte AWS, nous vous recommandons de vérifier si votre compte approche du quota pour les rôles IAM. Pour plus d'informations, voirQuotas 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, voirDemande d'augmentation de quotadans leGuide de l'utilisateur des quotas de service.

Pare-feux et passerelles Web sécurisées de nouvelle génération

Si vous filtrez l'accès à des informations spécifiquesAWSdomaines 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/login
- https ://*[votre région]*.signin.aws/plateform/login

Utilisation de plusieurs Comptes AWS

Comptes AWSservir de frontière de sécurité fondamentale dansAWS. 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 plusieursComptes AWSvous 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 auditeurCompte AWSqui héberge tous les éléments de votre charge de travail soumis àNormes de sécurité du secteur des cartes de paiement (PCI).
- Isolement— UnCompte AWSest une unité de protection de sécurité. Les risques potentiels et les menaces de sécurité doivent être contenus dans unCompte AWSsans 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 séparantComptes 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 laRèglement 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 plusieursComptes 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 utilisantAWS Organizationset facturation consolidée) tout en séparant les rubriques parCompte AWS.
- Allocation de quotas—AWSles quotas de service sont appliqués séparément pour chacunCompte AWS. Séparer les charges de travail en différentesComptes AWSles empêche de consommer des quotas les uns pour les autres.

Toutes les recommandations et procédures décrites dans ce guide sont conformes à laAWSUn 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'utiliserAWS Organizations, qui est gratuitAWSservice, pour gérer tous lesComptes AWSdans votre organisation.

AWSpropose égalementAWS Control Tower, qui ajoute des couches deAWSgestion de l'automatisation aux organisations et l'intègre automatiquement à d'autresAWSdes services tels queAWS CloudTrail,AWS Config, AmazonCloudWatch,AWS Service Catalog, et d'autres. Ces services peuvent entraîner des coûts supplémentaires. Pour en savoir plus, consultez PricingAWS Control Tower (Tarification).

Partie 1 : Configuration d'un nouveauCompte AWS

Ces instructions vous aideront à créer unCompte AWSet sécurisez 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 : S'inscrire pour un compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. ChoisissezCréez unCompte AWS.

   > **Note**
   >
   > Si vous vous êtes connecté àAWSrécemment, choisissezConnectez-vous à la console. Si l'optionCréez un nouveauCompte AWSn'est pas visible, choisissez d'abordConnectez-vous à un autre compte, puis choisissezCréez un nouveauCompte AWS.

3. Entrez les informations de votre compte, puis choisissezPoursuivre.

   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. ChoisissezPersonnelouProfessionnel.

   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 dansExigences relatives à Compte AWS.
6. Lisez et acceptez leAWSContrat avec le client.
7. ChoisissezCréer un compte et continuer.

À ce stade, vous recevrez un e-mail confirmant que votreCompte AWSest 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 utiliserAWSservices jusqu'à ce que vous ayez fini d'activer votre compte.

8. Sur leInformations de paiementpage, 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, choisissezUtiliser une nouvelle adresseet entrez l'adresse que vous souhaitez utiliser à des fins de facturation.
9. ChoisissezVérifier 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 localeAWSvendeur 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. LeAWSun système de vérification automatique vous appelle et vous fournit un code PIN. Entrez le code PIN à l'aide de votre téléphone, puis choisissezPoursuivre.
12. Sélectionnez unAWS Supportplan.

    Pour une description des plans disponibles, voirComparezAWS Supportplans.

    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 nouveauCompte AWS. Jusqu'à ce que l'activation soit terminée, vous pouvez voir unInscription complètebouton. Vous pouvez l'ignorer.

    AWSenvoie 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 pour la première fois un Compte AWS, vous commencez avec une seule identité de connexion qui donne un accès complet à tous Services AWS et les ressources du compte. Cette identité s'appelle Compte AWS utilisateur 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 nécessitent que vous vous connectiez en tant qu'utilisateur root, consultez la section Tâches nécessitant des informations d'identification utilisateur root dans le Guide de IAM l'utilisateur.

Pour vous connecter en tant qu'utilisateur root

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

   > **Note**
   >
   > Si vous vous êtes déjà connecté en tant qu'utilisateur root dans ce navigateur, celui-ci se souvient peut-être de l'adresse e-mail du Compte AWS.
   > Si vous vous êtes déjà connecté en tant qu'IAMutilisateur à l'aide de ce navigateur, celui-ci peut afficher la page de connexion de IAM l'utilisateur 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 votre Compte AWS adresse e-mail associée à votre compte et cliquez sur 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 MFA pour votre Compte AWS utilisateur root

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 AWS. Étant 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. Plusieurs types de MFA sont disponibles.

Pour obtenir des instructions sur l'activation MFA pour l'utilisateur root, voir Activation d'MFAappareils 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 terminéPartie 1 : Configuration d'un nouveauCompte AWS, les étapes suivantes vous aideront à configurerCompte AWSaccès 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 unCompte AWSet créez un utilisateur administratif dans IAM Identity Center. Pour plus d'informations, voirPour démarrerdans leAWS IAM Identity CenterGuide de l'utilisateur.

Rubriques

Étape 1 : activer IAM Identity Center

> **Note**
>
> Si vous n'avez pas activé l'authentification multifactorielle (MFA) pour votre utilisateur root, complétezÉtape 3 : Activez MFA pour votre Compte AWS utilisateur rootavant 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 leConsole IAM Identity Center.
3. SousActiver IAM Identity Center, choisissezActiver.
4. IAM Identity Center nécessiteAWS Organizations. Si vous n'avez pas encore créé d'organisation, vous devez choisir d'avoirAWScréez-en un pour vous. ChoisissezCréezAWSorganisationpour terminer ce processus.

   AWS Organizationsenvoie 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 dansAWS Organizations. Pour plus d'informations, voirAdministration déléguéedans leAWS IAM Identity CenterGuide 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 votreCompte 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 leurComptes AWSet applications.

Rubriques

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 unAWS Managed Microsoft ADun répertoire, un annuaire autogéré dans Active Directory ou un IdP externe avec IAM Identity Center. Si vous envisagez de connecter unAWS Managed Microsoft ADrépertoire ou annuaire autogéré dans Active Directory, assurez-vous que votre configuration Active Directory répond aux conditions requises dansActive Directory ou IdP externe.

> **Note**
>
> Pour des raisons de sécurité, nous vous recommandons vivement d'activer l'authentification multifactorielle. Si vous envisagez de connecter unAWS Managed Microsoft ADrépertoire ou répertoire autogéré dans Active Directory et vous n'utilisez pas RADIUS MFA avecAWS 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 desIdPs. Pour plus d'informations, voirActiver le MFAdans leAWS IAM Identity CenterGuide de l'utilisateur.

AWS Managed Microsoft AD

1. Consultez les directives figurant dansSe connecter à un Microsoft Active Directory.
2. Suivez les étapes décrites dansConnecter un répertoire dansAWS Managed Microsoft ADvers 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, voirSynchroniser un utilisateur administratif dans IAM Identity Center.

Répertoire autogéré dans Active Directory

1. Consultez les directives figurant dansSe connecter à un Microsoft Active Directory.
2. Suivez les étapes décrites dansConnecter 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, voirSynchroniser un utilisateur administratif dans IAM Identity Center.

IdP externe

1. Consultez les directives figurant dansConnectez-vous à un fournisseur d'identité externe.
2. Suivez les étapes décrites dansComment 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 leConsole IAM Identity Center.
2. Sélectionnez Settings (Paramètres).
3. Sur leRéglagespage, choisissezSource d'identitéonglet, choisissezActions, puis choisissezGérer la synchronisation.
4. Sur leGérer la synchronisationpage, choisissezUtilisateursonglet, puis choisissezAjouter des utilisateurs et des groupes.
5. Sur leUtilisateursonglet, sousUtilisateur, entrez le nom d'utilisateur exact et choisissezAjouter.
6. SousUtilisateurs 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 leGérer la synchronisationpage, l'utilisateur que vous avez spécifié apparaît dansUtilisateurs dans le périmètre de synchronisationliste.
8. Dans le panneau de navigation, choisissez utilisateurs.
9. Sur leUtilisateurs, 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 leConsole IAM Identity Center.
3. Suivez les étapes décrites dansAjouter des utilisateurspour 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'objetInvitation à adhérerAWSAuthentification unique. Ouvrez l'e-mail et choisissezAccepter l'invitation.

   b. Sur leInscription d'un nouvel utilisateurpage, entrez et confirmez un mot de passe, puis choisissezDéfinir un nouveau mot de passe.

   > **Note**
   >
   > Assurez-vous d'enregistrer votre mot de passe. Vous en aurez besoin plus tard pourÉtape 5 : Connectez-vous auAWSaccédez 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 àCompte 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 leConsole IAM Identity Center.
3. Dans le volet de navigation d'IAM Identity Center, sousAutorisations multi-comptes, choisissezEnsembles d'autorisations.
4. Choisissez Create permission set (Créer un jeu d'autorisations).
5. PourÉtape 1 : Sélectionnez le type d'ensemble d'autorisations, sur leSélectionnez le type d'ensemble d'autorisationspage, conservez les paramètres par défaut et choisissezSuivant. Les paramètres par défaut accordent un accès complet àAWSservices et ressources utilisantAdministratorAccessensemble d'autorisations prédéfini.

   > **Note**
   >
   > Le prédéfiniAdministratorAccessle jeu d'autorisations utiliseAdministratorAccess AWSpolitique gérée.

6. PourÉtape 2 : Spécifier les détails de l'ensemble d'autorisations, sur leSpécifier les détails de l'ensemble d'autorisationspage, conservez les paramètres par défaut et choisissezSuivant. Le paramètre par défaut limite votre session à une heure.
7. PourÉtape 3 : Révision et création, sur leRévision et créationpage, procédez comme suit :

   1. Vérifiez le type d'ensemble d'autorisations et confirmez qu'il estAdministratorAccess.
   2. Passez en revue leAWSpolitique gérée et confirmez qu'elle l'estAdministratorAccess.

3. Sélectionnez Create (Créer).

Étape 4 : ConfigurationCompte AWSaccès pour un utilisateur administratif

Pour configurerCompte AWSaccès pour un utilisateur administratif dans IAM Identity Center, vous devez attribuer à l'utilisateurAdministratorAccessensemble 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 leConsole IAM Identity Center.
3. Dans le volet de navigation, sousAutorisations multi-comptes, choisissezComptes AWS.
4. Sur leComptes AWS, une liste arborescente de votre organisation s'affiche. Cochez la case située à côté duCompte AWSauquel vous souhaitez attribuer un accès administratif. Si votre organisation possède plusieurs comptes, cochez la case à côté du compte de gestion.
5. ChoisissezAttribuer des utilisateurs ou des groupes.
6. PourÉtape 1 : Sélection des utilisateurs et des groupes, sur leAttribuez des utilisateurs et des groupes à »***AWS-nom-compte***«page, procédez comme suit :

    1. Sur leUtilisateursonglet, 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, choisissezSuivant.
7. PourÉtape 2 : Sélection des ensembles d'autorisations, sur leAttribuer des ensembles d'autorisations à »***AWS-nom-compte***«page, sousEnsembles d'autorisations, sélectionnez leAdministratorAccessensemble d'autorisations.
8. Choisissez Suivant.
9. PourÉtape 3 : Révision et soumission, sur leVérifiez et soumettez les devoirs à »***AWS-nom-compte***«page, procédez comme suit :

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

2. Après avoir vérifié que le bon utilisateur est affecté auAdministratorAccessensemble d'autorisations, choisissezSoumettre.

> **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 situations suivantes s'applique, suivez les étapes décrites dansActiver le MFApour activer la MFA pour IAM Identity Center :

- Vous utilisez le répertoire Identity Center par défaut comme source d'identité.
- Vous utilisez unAWS Managed Microsoft ADrépertoire ou répertoire autogéré dans Active Directory comme source d'identité et vous n'utilisez pas RADIUS MFA avecAWS 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 externesIdPs.

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

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

Procédez comme suit pour confirmer que vous pouvez vous connecter auAWSaccédez au portail en utilisant les informations d'identification de l'utilisateur administratif et que vous pouvez accéder auCompte 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 àhttps://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 leAWSaccédez 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 au`AdministratorAccess`ensemble d'autorisations, le rôle apparaîtra dansAWSaccéder 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 problèmesCompte AWSproblèmes de création

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

Problèmes

- Je n'ai pas reçu l'appel deAWSpour vérifier mon nouveau compte
- Je reçois un message d'erreur concernant le « nombre maximum de tentatives infructueuses » lorsque j'essaie de vérifier monCompte AWSpar téléphone
- Cela fait plus de 24 heures et mon compte n'est pas activé

Je n'ai pas reçu l'appel deAWSpour vérifier mon nouveau compte

Lorsque vous créez unCompte 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 votremode de paiementest correct.

Si vous n'avez pas reçu de SMS ou d'appel pour terminer le processus de vérification d'identité,AWS Supportpeut vous aider à activer votreCompte AWSmanuellement. Procédez comme suit :

1. Assurez-vous d'être joignable aunuméro de téléphoneque vous avez fourni pour votreCompte AWS.
2. Ouvrez leAWS Supportconsole, puis choisissezCréer un dossier.
   a. Choisissez Support de compte et facturation.
   b. PourType, sélectionnezCompte.

c. PourCatégorie, sélectionnezActivation.

d. Dans leDescription du cassection, indiquez la date et l'heure auxquelles vous pouvez être contacté.

e. Dans leOptions de contactsection, sélectionnezDiscuterpourMéthodes de contact.

f. Sélectionnez Submit (Envoyer).

> **Note**
>
> Vous pouvez créer un dossier avecAWS Supportmême si votreCompte AWSn'est pas activé.

Je reçois un message d'erreur concernant le « nombre maximum de tentatives infructueuses » lorsque j'essaie de vérifier monCompte AWSpar téléphone

AWS Supportpeut vous aider à activer manuellement votre compte. Procédez comme suit :

1. Connectez-vous à votreCompte AWSen utilisant l'adresse e-mail et le mot de passe que vous avez spécifiés lors de la création de votre compte.
2. Ouvrez leAWS Supportconsole, puis choisissezCréer un dossier.
3. ChoisissezAssistance relative aux comptes et à la facturation.
4. PourType, sélectionnezCompte.
5. PourCatégorie, sélectionnezActivation.
6. Dans leDescription du cassection, indiquez la date et l'heure auxquelles vous pouvez être contacté.
7. Dans leOptions de contactsection, sélectionnezDiscuterpourMéthodes de contact.
8. Sélectionnez Submit (Envoyer).

AWS Supportvous contactera et tentera d'activer manuellement votreCompte 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 leenregistrementpage. ChoisissezConnectez-vous à un compte existantCompte 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 leAWS Billing and Cost Managementconsole, vérifierModes de paiementpour les erreurs.
- Contactez votre institution financière.

  Parfois, les institutions financières rejettent les demandes d'autorisation émanant deAWS. Contactez l'établissement associé à votre mode de paiement et demandez-lui d'approuver les demandes d'autorisation émanant deAWS.AWSannule 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.
- ContacterAWS Support.

  ContacterAWS Supportpour 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 avecAWS.

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.