Guide de référence

AWS Gestion du compte

AWS Gestion du compte: Guide de référence

Table of Contents

Bienvenue dans le guide de référence AWS sur la gestion des comptes

Comptes AWSconstituent un élément fondamental de l'accès aux AWS services.

An Compte AWS remplit deux fonctions de base :

- Conteneur — An Compte AWS est le conteneur de base pour toutes les AWS ressources que vous créez en tant que AWS client. Par exemple, un bucket Amazon Simple Storage Service (Amazon S3), une base de données Amazon Relational Database Service (Amazon RDS) et une instance Amazon Elastic Compute Cloud (Amazon EC2) sont tous des ressources. Chaque ressource est identifiée de manière unique par un Amazon Resource Name (ARN) qui inclut l'ID de compte du compte qui contient ou possède la ressource.
- Limite de sécurité — An Compte AWS est également la limite de sécurité de base pour vos AWS ressources. Les ressources que vous créez dans votre compte sont accessibles aux utilisateurs disposant des informations d'identification associées à votre compte.

  Parmi les principales ressources que vous pouvez créer dans votre compte figurent les identités, telles que les utilisateurs et les rôles. Les identités comportent des informations d'identification que quelqu'un peut utiliser pour se connecter (s'authentifierAWS). Les identités ont également des politiques d'autorisation qui spécifient ce qu'un utilisateur peut faire (autorisation) avec les ressources du compte.

  Pour des raisons de sécurité, demandez à vos utilisateurs d'utiliser des informations d'identification temporaires lors de l'accèsAWS. Pour fournir des informations d'identification temporaires, vous pouvez utiliser la fédération et un fournisseur d'identité, tel que AWS IAM Identity Center(IAM Identity Center). Si votre entreprise utilise déjà un fournisseur d'identité, utilisez-le avec la fédération afin de simplifier la manière dont vous fournissez l'accès aux ressources de votreCompte AWS.

  Pour plus d'informations sur les meilleures pratiques de sécurité, consultez la section Bonnes pratiques de sécurité dans IAM dans le guide de l'utilisateur IAM.

Rubriques

- Utilisation du Utilisateur racine d'un compte AWS

Ai-je besoin de plusieursComptes AWS?

Comptes AWSservent de frontière fondamentale en matière de sécurité dansAWS. Ils servent de conteneur de ressources offrant un niveau d'isolement utile. La capacité d'isoler les ressources et les utilisateurs est essentielle pour établir un environnement sécurisé et bien gouverné.

Séparation de vos ressources en ressources séparéesComptes AWSvous aide à prendre en charge les principes suivants dans votre environnement cloud :

- Contrôle de sécurité— Différentes applications peuvent avoir des profils de sécurité différents, nécessitant des politiques et mécanismes de contrôle différents autour d'elles. Par exemple, il est beaucoup plus facile de parler à un auditeur et d'être en mesure de pointer vers un seulCompte AWSqui héberge tous les éléments de votre charge de travail soumis àNormes de sécurité PCI (Payment Card Industry).
- Isolation— UnCompte AWSest une unité de protection de sécurité. Les risques potentiels et les menaces à la sécurité devraient être contenus dans unCompte AWSsans affecter les autres. Il peut y avoir des besoins de sécurité différents en raison de différentes équipes ou de différents profils de sécurité.
- De nombreuses équipes— Les différentes équipes ont leurs responsabilités et leurs besoins en ressources différents. Vous pouvez empêcher les équipes d'interférer les unes avec les autres en les déplaçant pour les séparer.Comptes AWS.
- ISOLATION DES DONNÉES— En plus d'isoler les équipes, il est important d'isoler les banques de données dans un compte. Cela peut aider à limiter le nombre de personnes qui peuvent accéder à ce magasin de données et le gérer. Cela permet de limiter l'exposition à des données hautement privées et peut donc contribuer au respect de laRèglement général sur la protection des données (RGPR) de l'Union européenne.
- Processus métier— Différentes unités commerciales ou produits 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 moyen de séparer les articles au niveau de la facturation. Plusieurs comptes permettent de séparer les éléments au niveau de la facturation entre les unités commerciales, les équipes fonctionnelles ou les utilisateurs individuels. Vous pouvez toujours consolider toutes vos factures à un seul payeur (en utilisantAWS Organizationset facturation consolidée) tout en ayant des lignes séparées parCompte AWS.

- Allocation de quotas–AWSles quotas de service sont appliqués séparément pour chaqueCompte AWS. Séparation des charges de travail en différentesComptes AWSles empêche de consommer des quotas les uns pour les autres.

Toutes les recommandations et procédures décrites dans ce document sont conformes à laAWSCadre Well-Architected. Ce cadre est destiné à vous aider à concevoir une infrastructure cloud flexible, résiliente et évolutive. Même lorsque vous commencez petit, nous vous recommandons de suivre ces directives dans le 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.

Gestion de plusieursComptes AWS

Avant de commencer à ajouter plusieurs comptes, vous devez développer un plan pour les gérer. Pour cela, nous vous recommandons d'utiliserAWS Organizations, qui est gratuitAWSservice pour gérer tous lesComptes AWSdans votre organisation.

AWSoffre égalementAWS Control Tower, qui ajoute des couches deAWSautomatisation gérée aux Organizations et l'intègre automatiquement à d'autresAWSservices tels queAWS CloudTrail,AWS ConfigAmazon CloudWatch,AWS Service Catalog, et d'autres. Ces services peuvent entraîner des frais supplémentaires. Pour en savoir plus, consultez Tarification de AWS Control Tower.

Mise en route : vous en êtes un AWS utilisateur pour la première fois ?

Si vous utilisez pour la première foisAWS, la première étape consiste à vous inscrire à unCompte AWS. Lorsque vous vous inscrivez, AWS créez un compte Compte AWS avec les informations que vous fournissez et vous attribuez le compte. Après avoir créé votreCompte AWS, connectez-vous en tant qu'utilisateur root, activez l'authentification multifactorielle (MFA) pour l'utilisateur root et attribuez un accès administratif à un utilisateur.

Étapes

- Prérequis
- Étape 1 : Créez votre Compte AWS
- Étape 2 : activer le MFA pour votre utilisateur root
- Étape 3 : créer un utilisateur administrateur
- Rubriques en relation

Prérequis

Pour vous inscrire à unCompte AWS, vous avez besoin des informations suivantes :

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

  Nous vous recommandons d'utiliser une méthode standard pour nommer vos comptes afin de pouvoir leur attribuer des noms faciles à reconnaître. Pour les comptes d'entreprise, pensez à utiliser une norme de dénomination telle que organisation - objectif - environnement (par exemple, AnyCompany- audit - production). Pour les comptes personnels, pensez à utiliser une norme de dénomination telle que prénom, nom de famille, objectif (par exemple, paulo-santos-testaccount).

  Pour plus d'informations sur la modification du nom d'un compte, voir Comment modifier le nom inscrit sur mon compte Compte AWS ? .
- Adresse — Si votre adresse de contact se trouve en Inde, le contrat d'utilisation de votre compte est conclu avec Amazon Internet Services Private Limited (AISPL), un AWS vendeur local en Inde. Vous devez fournir votre valeur CVV dans le cadre du processus de vérification. Il se peut également que vous deviez saisir un mot de passe à usage unique, selon votre banque. AISPL facture 2 INR à votre mode de paiement dans le cadre du processus de vérification. AISPL rembourse le montant de 2 INR une fois la vérification terminée.
- Une adresse e-mail — L'adresse e-mail est utilisée comme nom de connexion pour l'utilisateur root et est requise pour la restauration du compte. Vous devez être en mesure de recevoir les e-mails envoyés à cette adresse. Avant de pouvoir effectuer certaines tâches, vous devez vérifier que vous avez accès au courrier électronique envoyé à cette adresse.

  > **Important**
  >
  > Si ce compte est destiné à une entreprise, utilisez une liste de distribution d'entreprise sécurisée (par exemple,`it.admins@example.com`) afin que votre entreprise puisse y accéder Compte AWS même lorsqu'un employé change de poste ou quitte l'entreprise. Comme l'adresse e-mail peut être utilisée pour réinitialiser les informations d'identification de l'utilisateur root du compte, protégez l'accès à cette liste ou adresse de distribution.
- Un numéro de téléphone — Ce numéro peut être utilisé pour confirmer la propriété de votre compte. Vous devez être en mesure de recevoir des appels à ce numéro de téléphone.

> **Important**
>
> Si ce compte est destiné à une entreprise, utilisez un numéro de téléphone professionnel afin que votre entreprise puisse y accéder Compte AWS même lorsqu'un employé change de poste ou quitte l'entreprise.

Étape 1 : Créez votre Compte AWS

1. Dans votre navigateur, ouvrez la page d'AWSaccueil.
2. Choisissez Créer un Compte AWS.

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

3. Entrez les informations de votre compte, puis choisissez Vérifier l'adresse e-mail. Cela enverra un code de vérification à l'adresse e-mail que vous avez spécifiée.
4. Entrez votre code de vérification, puis choisissez Vérifier.
5. Entrez un mot de passe sécurisé pour votre utilisateur root, confirmez-le, puis choisissez Continuer. AWSnécessite que votre mot de passe remplisse les conditions suivantes :

   - Il doit comporter un minimum de 8 caractères et un maximum de 128 caractères.
   - Il doit inclure au moins trois des types de caractères suivants : majuscules, minuscules, chiffres et ! @ # $ % ^ & * () <> [] {} | _+-= symboles.
   - Il ne doit pas être identique à votre Compte AWS nom ou à votre adresse e-mail.

6. Choisissez Professionnel ou Personnel. La différence entre ces options réside dans les informations que nous vous demandons. Les deux types de comptes présentent les mêmes caractéristiques et fonctions.
7. Entrez vos informations professionnelles ou personnelles. Reportez-vous aux recommandations de la section Conditions préalables concernant l'adresse e-mail et le numéro de téléphone.
8. Lisez et acceptez le contrat AWS client. Assurez-vous de lire et de comprendre les termes du contrat AWS client.

9. Choisissez Continue (Continuer). À ce stade, vous recevrez un e-mail pour confirmer que votre appareil Compte AWS est prêt à être utilisé. Vous pouvez vous connecter à votre nouveau compte en utilisant l'adresse e-mail et le mot de passe que vous avez fournis lors de votre inscription. Cependant, vous ne pouvez utiliser aucun AWS service tant que vous n'avez pas terminé d'activer votre compte.
10. Entrez les informations relatives à votre mode de paiement. Si vous souhaitez utiliser une adresse différente à des fins de facturation, choisissez Utiliser une nouvelle adresse.
11. Choisissez Vérifier et continuer.
12. Entrez le code de votre pays ou de votre région dans la liste, puis entrez un numéro de téléphone auquel on pourra vous joindre dans les prochaines minutes. Entrez le code CAPTCHA et soumettez-le.
13. Lorsque le système automatique vous contacte, entrez le code PIN que vous avez reçu, puis soumettez-le.
14. Sélectionnez votre AWS Support plan. Pour une description des forfaits disponibles, voir Comparer les AWS Support forfaits.
15. Choisissez Terminer l'inscription. Une page de confirmation s'affiche pour indiquer que votre compte est en cours d'activation.
16. Vérifiez votre boîte de courrier électronique et votre dossier de courrier indésirable pour y trouver un message électronique confirmant l'activation de votre compte. L'activation prend généralement quelques minutes, mais peut parfois prendre jusqu'à 24 heures.

    Après avoir reçu le message d'activation, vous avez un accès complet à tous les AWS services.

> **Note**
>
> Si vous rencontrez des difficultés lors de l'activation de votre compte, consultezthe section called “Problèmes liés à la création de compte”.

Étape 2 : activer le MFA pour votre utilisateur root

Nous vous recommandons vivement d'activer le MFA pour votre utilisateur root. La MFA réduit considérablement le risque que quelqu'un accède à votre compte sans votre autorisation.

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.

   Pour obtenir de l'aide pour vous connecter en utilisant votre utilisateur root, voir Se connecter en AWS Management Console tant qu'utilisateur root dans le guide de l'utilisateur de AWS connexion.

2. Activez le MFA pour votre utilisateur root.

   Pour obtenir des instructions, consultez Activation d'un dispositif MFA virtuel pour l'utilisateur root de votre Compte AWS (console) dans le Guide de l'utilisateur IAM.

Étape 3 : créer un utilisateur administrateur

Dans la mesure où vous ne pouvez pas restreindre ce que peut faire un utilisateur root, nous vous recommandons vivement de ne pas utiliser votre utilisateur root pour des tâches qui ne l'exigent pas explicitement. Attribuez plutôt un accès administratif à un utilisateur administratif dans IAM Identity Center et connectez-vous en tant qu'utilisateur administratif pour effectuer vos tâches administratives quotidiennes.

Pour obtenir des instructions, voir Configurer Compte AWS l'accès pour un utilisateur administratif d'IAM Identity Center dans le guide de l'utilisateur d'IAM Identity Center.

Rubriques en relation

- Pour plus d'informations sur la protection des informations d'identification de l'utilisateur root, consultez la section Sécurisation des informations d'identification de l'utilisateur root dans le guide de l'utilisateur IAM.
- Pour obtenir la liste des tâches qui nécessitent l'utilisateur root, consultez la section Tâches nécessitant des informations d'identification de l'utilisateur root dans le guide de l'utilisateur IAM.

Utilisation du Utilisateur racine d'un compte AWS

> **Important**
>
> Toute personne qui dispose des informations d'identification d'utilisateur root pour votre Compte AWS dispose d'un accès illimité à toutes les ressources de votre compte, y compris aux informations de facturation.

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 éviter d'utiliser l'utilisateur root pour les tâches quotidiennes, découvrez comment configurer un utilisateur administratif dans AWS IAM Identity Center. Pour obtenir des recommandations de sécurité supplémentaires pour les utilisateurs root, consultez les meilleures pratiques pour les utilisateurs root pour votre Compte AWS.

Vous pouvez modifier ou réinitialiser le mot de passe de l'utilisateur root, et créer ou supprimer des clés d'accès (identifiants de clé d'accès et clés d'accès secrètes) pour votre utilisateur root. Pour obtenir de l'aide pour vous connecter en utilisant votre utilisateur root, voir Se connecter en AWS Management Console tant qu'utilisateur root dans le guide de l'utilisateur de AWS connexion.

Gérez votreCompte AWS

Cette section inclut des rubriques qui décrivent comment gérer votreCompte AWS.

> **Note**
>
> Si votreCompte AWSa été créé en Inde en utilisantAmazon Internet Services Private Limited(AISPL), d'autres considérations entrent en ligne de compte. Pour plus d'informations, veuillez consulter Gérer des comptes en Inde.

Rubriques

Création d'un appareil autonome Compte AWS

Cette rubrique explique comment créer un appareil autonome Compte AWS qui n'est pas géré parAWS Organizations. Si vous souhaitez créer un compte faisant partie d'une organisation gérée parAWS Organizations, consultez la section Création d'un compte membre dans votre organisation dans le Guide de AWS Organizations l'utilisateur.

Ces instructions concernent la création d'une zone Compte AWS en dehors de l'Inde. Pour créer un compte en Inde, voirCréez unCompte AWSavec AISPL.

AWS Management Console

Pour créer un Compte AWS

1. Ouvrez la page d'accueil d'Amazon Web Services.
2. Choisissez Créer un Compte AWS.

> **Note**
>
> Si vous vous êtes connecté AWS récemment, il est possible que cette option ne soit pas disponible. Choisissez plutôt Se connecter à la console. Ensuite, si Créer un nouveau compte n'est Compte AWS toujours pas visible, choisissez d'abord Se connecter à un autre compte, puis Créer un nouveau compteCompte AWS.

3. Entrez les informations de votre compte, puis choisissez Vérifier l'adresse e-mail. Cela enverra un code de vérification à l'adresse e-mail que vous avez spécifiée.

> **Important**
>
> En raison de la nature critique de l'utilisateur root du compte, nous vous recommandons vivement d'utiliser une adresse e-mail accessible à un groupe plutôt qu'à un individu uniquement. Ainsi, si la personne qui s'est inscrite Compte AWS quitte l'entreprise, elle Compte AWS peut toujours être utilisée car l'adresse e-mail est toujours accessible.
> Si vous perdez l'accès à l'adresse e-mail associée auCompte AWS, vous ne pourrez pas récupérer l'accès au compte si vous perdez le mot de passe.

4. Entrez votre code de vérification, puis choisissez Vérifier.
5. Entrez un mot de passe sécurisé pour votre utilisateur root, confirmez-le, puis choisissez Continuer. AWSnécessite que votre mot de passe remplisse les conditions suivantes :
   - Avoir un minimum de 8 caractères et un maximum de 128 caractères
   - Inclure au minimum trois des types de caractères suivants : majuscules, minuscules, chiffres, et les symboles ! @ # $ % ^ & * () <> [] {} | _ + - =
   - Ne pas être identique au nom ou à l'adresse e-mail de votre compte Compte AWS
6. Choisissez Professionnel ou Personnel. Les comptes personnels et les comptes professionnels présentent les mêmes caractéristiques et fonctions.

7. Entrez votre entreprise ou vos informations personnelles.

   > **Important**
   >
   > Pour les entreprisesComptes AWS, il est recommandé de saisir :
   >
   > - Un numéro de téléphone d'entreprise plutôt qu'un numéro de téléphone personnel.
   > - Une adresse e-mail avec un nom de domaine appartenant à l'entreprise ou à l'organisation qui utilisera le compte.
   >
   > La configuration de l'utilisateur root du compte avec une adresse e-mail individuelle ou un numéro de téléphone personnel peut rendre votre compte peu sûr.

8. Lisez et acceptez le contrat AWS client. Assurez-vous de lire et de comprendre les termes du contrat AWS client.
9. Choisissez Continue (Continuer). À ce stade, vous recevrez un e-mail pour confirmer que votre appareil Compte AWS est prêt à être utilisé. Vous pouvez vous connecter à votre nouveau compte en utilisant l'adresse e-mail et le mot de passe que vous avez fournis lors de votre inscription. Cependant, vous ne pouvez utiliser aucun AWS service tant que vous n'avez pas terminé d'activer votre compte.
10. Entrez les informations relatives à votre mode de paiement, puis choisissez Vérifier et continuer. Si vous souhaitez utiliser une adresse de facturation différente pour vos informations AWS de facturation, choisissez Utiliser une nouvelle adresse.

    Vous ne pouvez pas poursuivre le processus d'inscription tant que vous n'avez pas ajouté un mode de paiement valide.
11. Entrez le code de votre pays ou de votre région dans la liste, puis entrez un numéro de téléphone auquel on pourra vous joindre dans les prochaines minutes.
12. Entrez le code affiché dans le CAPTCHA, puis soumettez-le.
13. Lorsque le système automatique vous contacte, entrez le code PIN que vous avez reçu, puis soumettez-le.
14. Sélectionnez l'un des AWS Support forfaits disponibles. Pour une description des plans de Support disponibles et de leurs avantages, consultez la section Comparer les AWS Support plans.
15. Choisissez Terminer l'inscription. Une page de confirmation apparaît pour indiquer que votre compte est en cours d'activation.

16. Vérifiez votre boîte de courrier électronique et votre dossier de courrier indésirable pour y trouver un e-mail confirmant l'activation de votre compte. L'activation prend généralement quelques minutes, mais peut parfois prendre jusqu'à 24 heures.

    Après avoir reçu le message d'activation, vous avez un accès complet à tous les AWS services.

AWS CLI & SDKs

Vous pouvez créer des comptes membres dans une organisation gérée en AWS Organizations exécutant l'CreateAccountopération tout en étant connecté au compte de gestion de l'organisation.

Vous ne pouvez pas créer une entité autonome Compte AWS en dehors d'une organisation à l'aide d'une opération AWS Command Line Interface (AWS CLI) ou d'une AWS API.

Afficher les Compte AWS identifiants

AWS attribue les identifiants uniques suivants à chacun : Compte AWS

Compte AWS ID

Numéro à 12 chiffres, tel que 012345678901, qui identifie de manière unique un. Compte AWSDe nombreuses AWS ressources incluent l'ID de compte dans leurs Amazon Resource Names (ARN). La partie identifiant du compte distingue les ressources d'un compte des ressources d'un autre compte. Si vous êtes un utilisateur AWS Identity and Access Management (IAM), vous pouvez vous connecter à l' AWS Management Console aide de l'identifiant ou de l'alias du compte. Bien que les identifiants de compte, comme toute information d'identification, doivent être utilisés et partagés avec soin, ils ne sont pas considérés comme des informations secrètes, sensibles ou confidentielles.

ID utilisateur canonique

Un identifiant alphanumérique`79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be`, tel qu'une forme masquée de l'identifiant. Compte AWS Vous pouvez utiliser cet identifiant pour identifier et Compte AWS lorsque vous accordez un accès multicompte à des buckets et à des objets à l'aide d'Amazon Simple Storage Service (Amazon S3). Vous pouvez récupérer

l'ID utilisateur canonique de votre compte Compte AWS en tant qu'utilisateur root ou en tant qu'utilisateur IAM.

Vous devez être authentifié AWS pour consulter ces identifiants.

> **Warning**
>
> Ne communiquez pas vos AWS informations d'identification (y compris les mots de passe et les clés d'accès) à un tiers qui a besoin de vos Compte AWS identifiants pour partager AWS des ressources avec vous. Cela leur donnerait le même accès à celui Compte AWS que vous avez.

Trouvez votre Compte AWS identifiant

Vous pouvez trouver l' Compte AWS identifiant en utilisant le AWS Management Console ou le AWS Command Line Interface (AWS CLI). Dans la console, l'emplacement de l'ID de compte varie selon que vous êtes connecté en tant qu'utilisateur root ou en tant qu'utilisateur IAM. L'identifiant du compte est le même, que vous soyez connecté en tant qu'utilisateur root ou en tant qu'utilisateur IAM.

Trouver votre identifiant de compte en tant qu'utilisateur root

AWS Management Console

Pour trouver votre Compte AWS identifiant lorsque vous êtes connecté en tant qu'utilisateur root

> **Autorisations minimales**
>
> Pour effectuer les étapes suivantes, vous devez au moins disposer des autorisations IAM suivantes :
>
> - Lorsque vous vous connectez en tant qu'utilisateur root, vous n'avez besoin d'aucune autorisation IAM.

1. Dans la barre de navigation en haut à droite, choisissez le nom ou le numéro de votre compte, puis sélectionnez Security credentials.

> **Tip**
>
> Si vous ne voyez pas l'option Informations d'identification de sécurité, vous êtes peut-être connecté en tant qu'utilisateur fédéré avec un rôle IAM, plutôt qu'en tant qu'utilisateur IAM. Dans ce cas, recherchez le compte d'entrée et le numéro d'identification du compte à côté.

2. Dans la section Détails du compte, le numéro de compte apparaît à côté de l'Compte AWS ID.

AWS CLI & SDKs

Pour trouver votre Compte AWS identifiant à l'aide du AWS CLI

> **Autorisations minimales**
>
> Pour effectuer les étapes suivantes, vous devez au moins disposer des autorisations IAM suivantes :
>
> - Lorsque vous exécutez la commande en tant qu'utilisateur root, vous n'avez besoin d'aucune autorisation IAM.

Utilisez la commande get-caller-identity comme suit.

```
$ aws sts get-caller-identity \
    --query Account \
    --output text
123456789012
```

Trouvez votre identifiant de compte en tant qu'utilisateur IAM

AWS Management Console

Pour trouver votre Compte AWS identifiant lorsque vous êtes connecté en tant qu'utilisateur IAM

> **Autorisations minimales**
>
> Pour effectuer les étapes suivantes, vous devez au moins disposer des autorisations IAM suivantes :
>
> - `account:GetAccountInformation`

1. Dans la barre de navigation en haut à droite, choisissez votre nom d'utilisateur, puis sélectionnez Security credentials.

   > **Tip**
   >
   > Si vous ne voyez pas l'option Informations d'identification de sécurité, vous êtes peut-être connecté en tant qu'utilisateur fédéré avec un rôle IAM, plutôt qu'en tant qu'utilisateur IAM. Dans ce cas, recherchez le compte d'entrée et le numéro d'identification du compte à côté.

2. En haut de la page, sous Détails du compte, le numéro de compte apparaît à côté de Compte AWS ID.

AWS CLI & SDKs

Pour trouver votre Compte AWS identifiant à l'aide du AWS CLI

> **Autorisations minimales**
>
> Pour effectuer les étapes suivantes, vous devez au moins disposer des autorisations IAM suivantes :
>
> - Lorsque vous exécutez la commande en tant qu'utilisateur ou rôle IAM, vous devez disposer des éléments suivants :

- `sts:GetCallerIdentity`

Utilisez la commande get-caller-identity comme suit.

```
$ aws sts get-caller-identity \
    --query Account \
    --output text
123456789012
```

Trouvez l'identifiant d'utilisateur canonique pour votre Compte AWS

Vous pouvez trouver l'ID utilisateur canonique correspondant à votre Compte AWS utilisation du AWS Management Console ou du AWS CLI. L'ID utilisateur canonique d'un Compte AWS est spécifique à ce compte. Vous pouvez récupérer l'ID utilisateur canonique pour vous Compte AWS en tant qu'utilisateur root, utilisateur fédéré ou utilisateur IAM.

Trouvez l'ID canonique en tant qu'utilisateur root ou utilisateur IAM

AWS Management Console

Pour trouver l'ID utilisateur canonique de votre compte lorsque vous êtes connecté à la console en tant qu'utilisateur root ou utilisateur IAM

> **Autorisations minimales**
>
> Pour effectuer les étapes suivantes, vous devez au moins disposer des autorisations IAM suivantes :
>
> - Lorsque vous exécutez la commande en tant qu'utilisateur root, vous n'avez besoin d'aucune autorisation IAM.
> - Lorsque vous vous connectez en tant qu'utilisateur IAM, vous devez avoir :
>   - `account:GetAccountInformation`

1. Connectez-vous en AWS Management Console tant qu'utilisateur root ou en tant qu'utilisateur IAM.

2. Dans la barre de navigation en haut à droite, choisissez le nom ou le numéro de votre compte, puis sélectionnez Security credentials.

   > **Tip**
   >
   > Si vous ne voyez pas l'option Informations d'identification de sécurité, vous êtes peut-être connecté en tant qu'utilisateur fédéré avec un rôle IAM, plutôt qu'en tant qu'utilisateur IAM. Dans ce cas, recherchez le compte d'entrée et le numéro d'identification du compte à côté.

3. Dans la section Détails du compte, l'ID utilisateur canonique apparaît à côté de l'ID utilisateur canonique. Vous pouvez utiliser votre ID utilisateur canonique pour configurer les listes de contrôle d'accès (ACL) Amazon S3.

AWS CLI & SDKs

Pour trouver l'ID utilisateur canonique à l'aide du AWS CLI

La même commande AWS CLI d'API fonctionne pour les Utilisateur racine d'un compte AWSutilisateurs IAM ou les rôles IAM.

Utilisez la commande list-buckets comme suit.

```
$ aws s3api list-buckets \
    --query Owner.ID \
    --output text
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

Trouvez l'ID canonique en tant qu'utilisateur fédéré doté d'un rôle IAM

AWS Management Console

Pour trouver l'identifiant canonique de votre compte lorsque vous êtes connecté à la console en tant qu'utilisateur fédéré doté d'un rôle IAM

> **Autorisations minimales**
>
> - Vous devez être autorisé à répertorier et à consulter un compartiment Amazon S3.

1. Connectez-vous au en AWS Management Console tant qu'utilisateur fédéré doté d'un rôle IAM.
2. Dans la console Amazon S3, choisissez un nom de compartiment pour afficher les détails relatifs à un compartiment.
3. Choisissez l'onglet Permissions (Autorisations).
4. Dans la section Liste de contrôle d'accès, sous Propriétaire du compartiment, l'identifiant canonique de votre compte Compte AWS apparaît.

AWS CLI & SDKs

Pour trouver l'ID utilisateur canonique à l'aide du AWS CLI

La même commande AWS CLI d'API fonctionne pour les Utilisateur racine d'un compte AWSutilisateurs IAM ou les rôles IAM.

Utilisez la commande list-buckets comme suit.

```
$ aws s3api list-buckets \
    --query Owner.ID \
    --output text
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

Mettre à jour le Compte AWS nom, l'adresse e-mail ou le mot de passe de l'utilisateur root

Pour modifier votre Compte AWS nom, ou pour changer le mot de passe ou l'adresse e-mail de l'utilisateur root, suivez les étapes de la procédure suivante. Cette adresse e-mail et ce mot de passe sont les informations d'identification que vous utilisez pour vous connecter en tant que Utilisateur racine d'un compte AWS.

> **Note**
>
> Les modifications apportées à an Compte AWS peuvent prendre jusqu'à quatre heures pour se propager partout.

AWS Management Console

Pour modifier votre Compte AWS nom, votre mot de passe d'utilisateur root ou votre adresse e-mail d'utilisateur root

> **Autorisations minimales**
>
> Pour effectuer les étapes suivantes, vous devez au moins disposer des autorisations IAM suivantes :
>
> - Vous devez vous connecter en tant que Utilisateur racine d'un compte AWS, ce qui ne nécessite aucune autorisation IAM supplémentaire. Vous ne pouvez pas effectuer ces étapes en tant qu'utilisateur ou rôle IAM.

1. Utilisez votre Compte AWS adresse e-mail et votre mot de passe pour vous connecter en AWS Management Consoletant que votre Utilisateur racine d'un compte AWS.
2. Dans le coin supérieur droit de la console, choisissez votre nom ou votre numéro de compte, puis choisissez Compte.
3. Sur la page Compte, à côté de Paramètres du compte, choisissez Modifier. Pour des raisons de sécurité, vous êtes invité à vous réauthentifier.

   > **Note**
   >
   > Si l'option Modifier ne s'affiche pas, il est probable que vous ne soyez pas connecté en tant qu'utilisateur root de votre compte. Vous ne pouvez pas modifier les paramètres du compte lorsque vous êtes connecté en tant qu'utilisateur ou rôle IAM.

4. Sur la page Mettre à jour les paramètres du compte, choisissez Modifier à côté du champ que vous souhaitez mettre à jour.

   a. Pour le nom — Sur la page Mettre à jour le nom de votre compte, dans Nouveau nom de compte, entrez le nouveau nom du compte, puis choisissez Enregistrer les modifications.

      > **Note**
      >
      > Si vous ne parvenez pas à modifier le Compte AWS nom, vérifiez s'il existe une politique de contrôle des services (SCP) AWS Organizations

qui restreint l'accès à l'action `account` ou est configurée pour refuser l'`iam:UpdateAccountName`action.

b. Pour les e-mails : sur la page Mettre à jour votre adresse e-mail, remplissez les champs Nouvelle adresse e-mail, Confirmez la nouvelle adresse e-mail et confirmez votre mot de passe actuel. Ensuite, choisissez Save changes (Enregistrer les modifications). Un code de vérification est envoyé à votre nouvelle adresse e-mail depuis`no-reply@verify.signin.aws`. Sur la page Vérifiez votre nouvelle adresse e-mail, sous Code de vérification, entrez le code que vous avez reçu de votre e-mail, puis choisissez Enregistrer les modifications.

> **Note**
>
> L'arrivée du code de vérification peut prendre jusqu'à 5 minutes. Si vous ne voyez pas l'e-mail dans votre boîte de réception, vérifiez vos dossiers de courrier indésirable et de courrier indésirable.

c. Pour le mot de passe — Sur la page Mettre à jour votre mot de passe, remplissez les champs Mot de passe actuel, Nouveau mot de passe et Confirmer le nouveau mot de passe. Ensuite, choisissez Save changes (Enregistrer les modifications). Pour obtenir des conseils supplémentaires, notamment sur les meilleures pratiques relatives à la définition des mots de passe des utilisateurs root, voir Modifier le Utilisateur racine d'un compte AWS mot de passe du guide de l'utilisateur IAM.

5. Lorsque vous avez apporté toutes vos modifications, choisissez Effectué.

AWS CLI & SDKs

Cette tâche n'est pas prise en charge dans AWS CLI ou par une opération d'API provenant de l'un des AWS SDK. Vous ne pouvez effectuer cette tâche qu'à l'aide du AWS Management Console.

Comprendre les modes de fonctionnement de l'API

Les opérations d'API qui fonctionnent avec unCompte AWSLes attributs de fonctionnent toujours selon l'un des deux modes de fonctionnement suivants :

- Contexte autonome— ce mode est utilisé lorsqu'un utilisateur ou un rôle d'un compte accède ou modifie un attribut de compte dans lemême compte. Le mode contextuel autonome est

automatiquement utilisé lorsque vousDon'tIncluez le`AccountId`lorsque vous appelez l'un des paramètres de gestion de compteAWS CLIouAWSLes opérations du SDK.

- Contexte Organizations— ce mode est utilisé lorsqu'un utilisateur ou un rôle d'un compte d'une organisation accède à un attribut de compte dans un autre compte membre de la même organisation ou le modifie. Le mode contextuel de l'organisation est automatiquement utilisé lorsque vousfaireIncluez le`AccountId`lorsque vous appelez l'un des paramètres de gestion de compteAWS CLIouAWSFonctionnement du SDK. Vous pouvez appeler les opérations dans ce mode uniquement à partir du compte de gestion de l'organisation ou du compte administrateur délégué pour la gestion de compte.

LeAWS CLIetAWSLes opérations du SDK peuvent fonctionner de manière autonome ou dans le contexte d'une organisation.

- Si vousDon'tIncluez le`AccountId`, puis l'opération s'exécute dans le contexte autonome et applique automatiquement la demande au compte que vous avez utilisé pour effectuer la demande. Cela est vrai que le compte soit membre ou non d'une organisation.
- Si vous incluez le`AccountId`, puis l'opération s'exécute dans le contexte des organisations et l'opération fonctionne sur le compte Organizations spécifié.
  - Si le compte appelant l'opération est le compte de gestion ou le compte d'administrateur délégué pour le service de gestion des comptes, vous pouvez spécifier n'importe quel compte de membre de cette organisation dans le`AccountId`pour mettre à jour le compte spécifié.
  - Le seul compte d'une organisation qui peut appeler l'une des autres opérations de contact et spécifier son propre numéro de compte dans le`AccountId`est le compte spécifié en tant quecompte administrateur déléguépour le service de gestion de compte. Tout autre compte, y compris le compte de gestion, reçoit un`AccessDenied`exception.
- Si vous exécutez une opération en mode autonome, vous devez être autorisé à exécuter l'opération avec une stratégie IAM qui inclut un`Resource`élément de`"*"`pour autoriser toutes les ressources, ouARN qui utilise la syntaxe d'un compte autonome.
- Si vous exécutez une opération en mode organisations, vous devez être autorisé à exécuter l'opération avec une stratégie IAM qui inclut un`Resource`élément de`"*"`pour autoriser toutes les ressources, ouARN qui utilise la syntaxe d'un compte de membre dans une organisation.

Autorisation de mise à jour des attributs de compte

Comme pour la plupartAWSopérations, vous accordez des autorisations pour ajouter, mettre à jour ou supprimer des attributs de compte pourComptes AWSen utilisantStratégies d'autorisations IAM. Lorsque vous associez une stratégie d'autorisation IAM à un principal IAM (utilisateur ou rôle), vous spécifiez les actions que le principal peut effectuer sur quelles ressources et dans quelles conditions.

Voici quelques considérations spécifiques à la gestion des comptes pour la création d'une stratégie d'autorisations.

Format Amazon Resource Name pourComptes AWS

- LeAmazon Resource Name (ARN)pour unCompte AWSque vous pouvez inclure dans`resource`d'une déclaration de stratégie est construit différemment selon que le compte que vous souhaitez référencer est un compte autonome ou un compte appartenant à une organisation. Voir la section précédente surComprendre les modes de fonctionnement de l'API.
  - Un ARN de compte pour un compte autonome :

    ```
    arn:aws:account::{AccountId}:account
    ```

    Vous devez utiliser ce format lorsque vous exécutez une opération d'attributs de compte en mode autonome en n'incluant pas le`AccountID` Paramètre .
  - Un ARN de compte pour un compte membre au sein d'une organisation :

    ```
    arn:aws:account::{ManagementAccountId}:account/o-{OrganizationId}/{AccountId}
    ```

    Vous devez utiliser ce format lorsque vous exécutez une opération d'attributs de compte en mode organisations en incluant le`AccountID` Paramètre .

Clés contextuelles pour les stratégies IAM

Le service de gestion de compte fournit également plusieursClés de condition spécifiques au service de gestion de comptequi fournissent un contrôle précis sur les autorisations que vous accordez.

`account:AccountResourceOrgPaths`

La clé contextuelle`account:AccountResourceOrgPaths`vous permet de spécifier un chemin dans la hiérarchie de votre organisation vers une unité organisationnelle (UO) spécifique. Seuls les comptes de membres contenus par cette unité d'organisation correspondent à la condition. L'exemple d'extrait suivant restreint la stratégie afin qu'elle ne s'applique qu'aux comptes qui se trouvent dans l'une des deux unités d'organisation spécifiées.

Etant donné que`account:AccountResourceOrgPaths`est un type de chaîne à plusieurs valeurs, vous devez utiliser la propriété`ForAnyValue`ou`ForAllValues`opérateurs de chaîne à valeurs multiples. Notez également que le préfixe de la clé de condition est`account`, même si vous faites référence aux chemins d'accès aux unités organisationnelles d'une organisation.

```
"Condition": {
    "ForAnyValue:StringLike": {
        "account:AccountResourceOrgPaths": [
            "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/*",
            "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h222/*"
        ]
    }
}
```

`account:AccountResourceOrgTags`

La clé contextuelle`account:AccountResourceOrgTags`vous permet de référencer les balises qui peuvent être associées à un compte dans une organisation. Une balise est une paire de chaînes clé/valeur que vous pouvez utiliser pour catégoriser et étiqueter les ressources de votre compte. Pour plus d'informations sur le balisage, consultezTag Editordans leAWS Resource GroupsGuide de l'utilisateur. Pour plus d'informations sur l'utilisation de balises dans le cadre d'une stratégie de contrôle d'accès basé sur les attributs, consultezQu'est-ce que le contrôle d'accès baséAWSdans leIAM User Guide. L'exemple d'extrait suivant restreint la stratégie afin qu'elle ne s'applique qu'aux comptes d'une organisation qui ont la balise avec la clé`project`et une valeur soit de`blueoured`.

Etant donné que`account:AccountResourceOrgTags`est un type de chaîne à plusieurs valeurs, vous devez utiliser la propriété`ForAnyValue`ou`ForAllValues`opérateurs de chaîne à valeurs multiples. Notez également que le préfixe de la clé de condition est`account`, même si vous faites référence aux balises du compte membre d'une organisation.

```
"Condition": {
```

```
    "ForAnyValue:StringLike": {
        "account:AccountResourceOrgTags/project": [
            "blue",
            "red"
        ]
    }
}
```

> **Note**
>
> Vous ne pouvez associer des balises qu'à un compte d'une organisation. Vous ne pouvez pas attacher de balises à un appareil autonomeCompte AWS.

Mettez à jour votreCompte AWSinformations de contact

Vous pouvez enregistrer les informations de contact concernantcontact principal du comptepour votreCompte AWS. Vous pouvez également ajouter ou modifier les informations de contact suivantescontacts du compte alternatif:

- Facturation— Le contact de facturation alternatif recevra des notifications relatives à la facturation, telles que des notifications de disponibilité des factures.
- Opérations— Le contact opérationnel alternatif recevra les notifications relatives aux opérations.
- Sécurité— Le contact de sécurité alternatif recevra des notifications relatives à la sécurité, y compris des notifications provenant duAWSÉquipe de lutte contre les abus.

Rubriques

- Mettez à jour les contacts alternatifs pour votre Compte AWS
- Mettez à jour le contact principal de votre Compte AWS

Mettez à jour les contacts alternatifs pour votre Compte AWS

Les contacts alternatifs AWS permettent de contacter jusqu'à trois autres contacts associés au compte. Il n'est pas nécessaire qu'un autre contact soit une personne en particulier. Il est également possible d'ajouter une liste de distribution par courrier électronique si vous avez une équipe qui gère la facturation, les opérations et les questions liées à la sécurité. Elles s'ajoutent à l'adresse e-mail

associée à l'utilisateur root du compte. Le contact principal du compte continuera de recevoir toutes les communications par e-mail envoyées à l'adresse e-mail du compte root.

Vous ne pouvez spécifier qu'un seul des types de contact suivants associés à un compte.

- Contact de facturation
- Contact des opérations
- Contact en matière de sécurité

Vous pouvez ajouter ou modifier des contacts alternatifs différemment, selon que les comptes sont autonomes ou font partie d'une organisation :

- Autonome Comptes AWS : si vous n'êtes Comptes AWS pas associé à une organisation, vous pouvez mettre à jour vos propres contacts alternatifs à l'aide de la console AWS de gestion, ou via la AWS CLI et les SDK. Pour savoir comment procéder, voir Mettre à jour les contacts Compte AWS secondaires autonomes.
- Comptes AWS au sein d'une organisation — Pour les comptes membres faisant partie d'une AWS organisation, un utilisateur du compte de gestion ou du compte administrateur délégué peut mettre à jour de manière centralisée n'importe quel compte membre de l'organisation depuis la AWS Organizations console ou par programmation via la AWS CLI et les SDK. Pour savoir comment procéder, voir Mettre à jour les contacts Compte AWS alternatifs dans votre organisation.

Rubriques

- Exigences relatives au numéro de téléphone et à l'adresse e-mail
- Mettre à jour les contacts secondaires pour un appareil autonome Compte AWS
- Mettez à jour les contacts alternatifs de tous Compte AWS les contacts de votre organisation
- compte : clé de AlternateContactTypes contexte

Exigences relatives au numéro de téléphone et à l'adresse e-mail

Avant de procéder à la mise à jour des informations de contact secondaires de votre compte, nous vous recommandons de vérifier les exigences suivantes lors de la saisie des numéros de téléphone et des adresses e-mail.

- Les numéros de téléphone ne peuvent contenir que des chiffres, des espaces et les caractères suivants : » +-( ) ».

- Les adresses e-mail peuvent comporter jusqu'à 254 caractères et peuvent inclure les caractères spéciaux suivants dans la partie locale de l'adresse e-mail, en plus des caractères alphanumériques standard : « `+=.#|!&-_` ».

Mettre à jour les contacts secondaires pour un appareil autonome Compte AWS

Pour ajouter ou modifier les contacts secondaires d'un appareil autonome Compte AWS, suivez les étapes de la procédure suivante. La AWS Management Console procédure ci-dessous ne fonctionne toujours que dans le contexte autonome. Vous pouvez utiliser le AWS Management Console pour accéder ou modifier uniquement les autres contacts du compte que vous avez utilisé pour appeler l'opération.

AWS Management Console

Pour ajouter ou modifier les contacts secondaires d'un appareil autonome Compte AWS

> **Autorisations minimales**
>
> Pour effectuer les étapes suivantes, vous devez au moins disposer des autorisations IAM suivantes :
>
> - `account:GetAlternateContact`(pour voir les autres coordonnées)
> - `account:PutAlternateContact`(pour définir ou mettre à jour un autre contact)
> - `account:DeleteAlternateContact`(pour supprimer un autre contact)

1. Connectez-vous en AWS Management Consoletant qu'utilisateur ou en tant que rôle IAM disposant des autorisations minimales.
2. Choisissez le nom de votre compte en haut à droite de la fenêtre, puis sélectionnez Compte.
3. Sur la page Compte, faites défiler la page vers le bas jusqu'à Autres contacts, puis à droite du titre, choisissez Modifier.

> **Note**
>
> Si l'option Modifier n'apparaît pas, il est probable que vous ne soyez pas connecté en tant qu'utilisateur root de votre compte ou en tant que personne disposant des autorisations minimales spécifiées ci-dessus.

4. Modifiez les valeurs de l'un des champs disponibles.

> **Important**
>
> Pour les entreprises Comptes AWS, il est recommandé de saisir le numéro de téléphone et l'adresse e-mail de l'entreprise plutôt que ceux d'un individu.

5. Après avoir effectué toutes les modifications, choisissez Mettre à jour.

AWS CLI & SDKs

Vous pouvez récupérer, mettre à jour ou supprimer les informations de contact secondaires à l'aide des AWS CLI commandes suivantes ou de leurs opérations équivalentes dans le AWS SDK :

- GetAlternateContact
- PutAlternateContact
- DeleteAlternateContact

> **Remarques**
>
> - Pour effectuer ces opérations à partir du compte de gestion ou d'un compte administrateur délégué d'une organisation sur les comptes des membres, vous devez activer l'accès sécurisé pour le service Account.

> **Autorisations minimales**
>
> Pour chaque opération, vous devez disposer de l'autorisation correspondant à cette opération :

- `GetAlternateContact`(pour voir les autres coordonnées)
- `PutAlternateContact`(pour définir ou mettre à jour un autre contact)
- `DeleteAlternateContact`(pour supprimer un autre contact)

Si vous utilisez ces autorisations individuelles, vous pouvez autoriser certains utilisateurs à lire uniquement les informations de contact, tandis que d'autres peuvent lire et écrire.

Example

L'exemple suivant permet de récupérer le contact alternatif de facturation actuel pour le compte de l'appelant.

```
$ aws account get-alternate-contact \
    --alternate-contact-type=BILLING
{
    "AlternateContact": {
        "AlternateContactType": "BILLING",
        "EmailAddress": "saanvi.sarkar@amazon.com",
        "Name": "Saanvi Sarkar",
        "PhoneNumber": "+1(206)555-0123",
        "Title": "CFO"
    }
}
```

Example

L'exemple suivant définit un nouveau contact alternatif des opérations pour le compte de l'appelant.

```
$ aws account put-alternate-contact \
    --alternate-contact-type=OPERATIONS \
    --email-address=mateo_jackson@amazon.com \
    --name="Mateo Jackson" \
    --phone-number="+1(206)555-1234" \
    --title="Operations Manager"
```

Cette commande ne produit aucune sortie si elle réussit.

Example

> **Note**
>
> Si vous effectuez plusieurs `PutAlternateContact` opérations sur le même Compte AWS type de contact, le premier ajoute le nouveau contact, et tous les appels successifs au même Compte AWS type de contact mettent à jour le contact existant.

Example

L'exemple suivant supprime le contact secondaire chargé de la sécurité pour le compte de l'appelant.

```
$ aws account delete-alternate-contact \
    --alternate-contact-type=SECURITY
```

Cette commande ne produit aucune sortie si elle réussit.

> **Note**
>
> Si vous essayez de supprimer le même contact plusieurs fois, le premier réussit silencieusement. Toutes les tentatives ultérieures génèrent une `ResourceNotFound` exception.

Mettez à jour les contacts alternatifs de tous Compte AWS les contacts de votre organisation

Pour ajouter ou modifier les coordonnées secondaires d'un membre Compte AWS de votre organisation, suivez les étapes de la procédure suivante.

Prérequis

Pour mettre à jour les contacts alternatifs avec la AWS Organizations console, vous devez définir certains paramètres préliminaires :

- Votre organisation doit activer toutes les fonctionnalités pour gérer les paramètres de vos comptes membres. Cela permet à l'administrateur de contrôler les comptes des membres. Ce paramètre est défini par défaut lorsque vous créez votre organisation. Si votre organisation est configurée pour la facturation consolidée uniquement et que vous souhaitez activer toutes les fonctionnalités, consultez la section Activation de toutes les fonctionnalités de votre organisation.
- Vous devez activer l'accès sécurisé pour le service de gestion des AWS comptes. Pour configurer cela, consultez la section Activation de l'accès sécurisé pour la gestion des AWS comptes.

> **Note**
>
> Les politiques AWS Organizations `AWSOrganizationsReadOnlyAccess` gérées `AWSOrganizationsFullAccess` sont mises à jour pour autoriser l'accès aux API de gestion des AWS comptes afin que vous puissiez accéder aux données du compte depuis la AWS Organizations console. Pour consulter les politiques gérées mises à jour, voir Mises à jour des politiques AWS gérées par les Organizations.

AWS Management Console

Pour ajouter ou modifier les contacts alternatifs de n'importe quel Compte AWS membre de votre organisation

1. Connectez-vous à la AWS Organizations console avec les informations d'identification du compte de gestion de l'organisation.
2. Dans Comptes AWS, sélectionnez le compte que vous souhaitez mettre à jour.
3. Choisissez Informations de contact, puis sous Autres contacts, recherchez le type de contact : contact de facturation, contact de sécurité ou contact opérationnel.
4. Pour ajouter un nouveau contact, sélectionnez Ajouter, ou pour mettre à jour un contact existant, sélectionnez Modifier.
5. Modifiez les valeurs de l'un des champs disponibles.

> **Important**
>
> Pour les entreprises Comptes AWS, il est recommandé de saisir le numéro de téléphone et l'adresse e-mail de l'entreprise plutôt que ceux d'un individu.

6. Après avoir effectué toutes les modifications, choisissez Mettre à jour.

AWS CLI & SDKs

Vous pouvez récupérer, mettre à jour ou supprimer les informations de contact secondaires à l'aide des AWS CLI commandes suivantes ou de leurs opérations équivalentes dans le AWS SDK :

- GetAlternateContact
- PutAlternateContact
- DeleteAlternateContact

> **Remarques**
>
> - Pour effectuer ces opérations à partir du compte de gestion ou d'un compte administrateur délégué d'une organisation sur les comptes des membres, vous devez activer l'accès sécurisé pour le service Account.
> - Vous ne pouvez pas accéder à un compte dans une organisation différente de celle que vous utilisez pour appeler l'opération.

> **Autorisations minimales**
>
> Pour chaque opération, vous devez disposer de l'autorisation correspondant à cette opération :
>
> - `GetAlternateContact`(pour voir les autres coordonnées)
> - `PutAlternateContact`(pour définir ou mettre à jour un autre contact)
> - `DeleteAlternateContact`(pour supprimer un autre contact)
>
> Si vous utilisez ces autorisations individuelles, vous pouvez autoriser certains utilisateurs à lire uniquement les informations de contact, tandis que d'autres peuvent lire et écrire.

Example

L'exemple suivant extrait le contact alternatif de facturation actuel pour le compte de l'appelant dans une organisation. Les informations d'identification utilisées doivent provenir du compte de gestion de l'organisation ou du compte administrateur délégué de la gestion des comptes.

```
$ aws account get-alternate-contact \
    --alternate-contact-type=BILLING \
    --account-id 123456789012
{
    "AlternateContact": {
        "AlternateContactType": "BILLING",
        "EmailAddress": "saanvi.sarkar@amazon.com",
        "Name": "Saanvi Sarkar",
        "PhoneNumber": "+1(206)555-0123",
        "Title": "CFO"
    }
}
```

Example

L'exemple suivant définit le contact alternatif des opérations pour le compte membre spécifié dans une organisation. Les informations d'identification utilisées doivent provenir du compte de gestion de l'organisation ou du compte administrateur délégué de la gestion des comptes.

```
$ aws account put-alternate-contact \
    --account-id 123456789012 \
    --alternate-contact-type=OPERATIONS \
    --email-address=mateo_jackson@amazon.com \
    --name="Mateo Jackson" \
    --phone-number="+1(206)555-1234" \
    --title="Operations Manager"
```

Cette commande ne produit aucune sortie si elle réussit.

> **Note**
>
> Si vous effectuez plusieurs `PutAlternateContact` opérations sur le même Compte AWS type de contact, le premier ajoute le nouveau contact, et tous les appels successifs au même Compte AWS type de contact mettent à jour le contact existant.

Example

L'exemple suivant supprime le contact secondaire chargé de la sécurité pour le compte membre spécifié dans une organisation. Les informations d'identification utilisées doivent provenir du compte de gestion de l'organisation ou du compte administrateur délégué de la gestion des comptes.

```
$ aws account delete-alternate-contact \
    --account-id 123456789012 \
    --alternate-contact-type=SECURITY
```

Cette commande ne produit aucune sortie si elle réussit.

Example

> **Note**
>
> Si vous essayez de supprimer le même contact plusieurs fois, le premier réussit silencieusement. Toutes les tentatives ultérieures génèrent une `ResourceNotFound` exception.

compte : clé de AlternateContactTypes contexte

Vous pouvez utiliser la clé de contexte `account:AlternateContactTypes` pour spécifier lequel des trois types de facturation est autorisé (ou refusé) par la politique IAM. Par exemple, l'exemple suivant de politique d'autorisation IAM utilise cette clé de condition pour permettre aux principaux rattachés de récupérer, mais pas de modifier, uniquement le contact `BILLING` alternatif pour un compte spécifique dans une organisation.

Comme il `account:AlternateContactTypes` s'agit d'un type de chaîne à valeurs multiples, vous devez utiliser les opérateurs `ForAnyValue`ou chaînes `ForAllValues` à valeurs multiples.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
```

```
            "Action": "account:GetAlternateContact",
            "Resource": [
                "arn:aws:account::123456789012:account/o-aa111bb222/111111111111"
            ],
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "account:AlternateContactTypes": [
                        "BILLING"
                    ]
                }
            }
        }
    ]
}
```

Mettez à jour le contact principal de votre Compte AWS

Vous pouvez mettre à jour les informations de contact principales associées à votre compte, notamment le nom complet, le nom de l'entreprise, l'adresse postale, le numéro de téléphone et l'adresse du site Web de votre contact.

Vous modifiez le contact principal du compte différemment, selon que les comptes sont autonomes ou font partie d'une organisation :

- Autonome Comptes AWS : si vous n'êtes Comptes AWS pas associé à une organisation, vous pouvez mettre à jour le contact principal de votre compte à l'aide de la console AWS de gestion ou via la AWS CLI et les SDK. Pour savoir comment procéder, voir Mettre à jour le contact Compte AWS principal autonome.
- Comptes AWSau sein d'une organisation — Pour les comptes membres faisant partie d'une AWS organisation, un utilisateur du compte de gestion ou du compte administrateur délégué peut mettre à jour de manière centralisée n'importe quel compte membre de l'organisation depuis la AWS Organizations console ou par programmation via la AWS CLI et les SDK. Pour savoir comment procéder, voir Mettre à jour le contact Compte AWS principal dans votre organisation.

Rubriques

- Exigences relatives au numéro de téléphone et à l'adresse e-mail
- Mettre à jour le contact principal pour un contact autonome Compte AWS
- Mettez à jour le contact principal de n'importe quel contact Compte AWS au sein de votre organisation

Exigences relatives au numéro de téléphone et à l'adresse e-mail

Avant de procéder à la mise à jour des informations de contact principales de votre compte, nous vous recommandons de vérifier les exigences suivantes lors de la saisie des numéros de téléphone et des adresses e-mail.

- Les numéros de téléphone ne peuvent contenir que des chiffres, des espaces et les caractères suivants : » + - ( ) ».
- Les numéros de téléphone doivent commencer par un code de pays + et ne doivent pas comporter de zéros ou d'espaces supplémentaires après le code de pays. Par exemple, +1 (États-Unis/Canada) ou +44 (Royaume-Uni).
- Les numéros de téléphone doivent inclure un trait d'union « - » entre le code régional, le code d'échange et le code local. Par exemple, +1 202-555-0179.

> **Note**
>
> Les numéros de téléphone saisis sans tiret peuvent empêcher la réception d'appels pendant le processus de vérification des numéros de téléphone lors de la réinitialisation d'un dispositif MFA pour l'utilisateur root. Pour plus d'informations, voir Comment réinitialiser le dispositif MFA de mon compte utilisateur AWS root ? .

- Pour des raisons de sécurité, les numéros de téléphone doivent pouvoir recevoir des SMSAWS. Les numéros sans frais ne seront pas acceptés car la plupart ne supportent pas les SMS.
- Pour les entreprisesComptes AWS, il est recommandé de saisir le numéro de téléphone et l'adresse e-mail de l'entreprise plutôt que ceux d'un individu. Si vous configurez l'utilisateur root du compte avec l'adresse e-mail ou le numéro de téléphone d'une personne, il peut être difficile de récupérer votre compte si cette personne quitte l'entreprise.

Mettre à jour le contact principal pour un contact autonome Compte AWS

Pour modifier vos coordonnées principales dans le cas d'un appareil autonomeCompte AWS, suivez les étapes de la procédure suivante. La AWS Management Console procédure ci-dessous ne fonctionne toujours que dans le contexte autonome. Vous pouvez utiliser le AWS Management Console pour accéder ou modifier uniquement les informations de contact principales du compte que vous avez utilisé pour appeler l'opération.

AWS Management Console

Pour modifier votre contact principal en tant que contact autonome Compte AWS

> **Autorisations minimales**
>
> Pour effectuer les étapes suivantes, vous devez au moins disposer des autorisations IAM suivantes :
>
> - `account:GetContactInformation`(pour voir les coordonnées principales)
> - `account:PutContactInformation`(pour mettre à jour les coordonnées principales)

1. Connectez-vous en AWS Management Consoletant qu'utilisateur ou en tant que rôle IAM disposant des autorisations minimales.
2. Choisissez le nom de votre compte en haut à droite de la fenêtre, puis sélectionnez Compte.
3. Faites défiler la page jusqu'à la section Informations de contact, puis choisissez Modifier.
4. Modifiez les valeurs de l'un des champs disponibles.
5. Une fois que vous avez apporté toutes vos modifications, choisissez Mettre à jour.

AWS CLI & SDKs

Vous pouvez récupérer, mettre à jour ou supprimer les informations de contact principales à l'aide des AWS CLI commandes suivantes ou de leurs opérations équivalentes dans le AWS SDK :

- GetContactInformation
- PutContactInformation

> **Remarques**
>
> - Pour effectuer ces opérations à partir du compte de gestion ou d'un compte administrateur délégué d'une organisation sur les comptes des membres, vous devez activer l'accès sécurisé pour le service Account.

Autorisations minimales

Pour chaque opération, vous devez disposer de l'autorisation correspondant à cette opération :

- `account:GetContactInformation`
- `account:PutContactInformation`

Si vous utilisez ces autorisations individuelles, vous pouvez autoriser certains utilisateurs à lire uniquement les informations de contact, tandis que d'autres peuvent lire et écrire.

Example

L'exemple suivant permet de récupérer les coordonnées principales actuelles du compte de l'appelant.

```
$ aws account get-contact-information
{
    "ContactInformation": {
        "AddressLine1": "123 Any Street",
        "City": "Seattle",
        "CompanyName": "Example Corp, Inc.",
        "CountryCode": "US",
        "DistrictOrCounty": "King",
        "FullName": "Saanvi Sarkar",
        "PhoneNumber": "+15555550100",
        "PostalCode": "98101",
        "StateOrRegion": "WA",
        "WebsiteUrl": "https://www.examplecorp.com"
    }
}
```

Example

L'exemple suivant définit les nouvelles informations de contact principales pour le compte de l'appelant.

```
$ aws account put-contact-information --contact-information \
'{"AddressLine1": "123 Any Street", "City": "Seattle", "CompanyName": "Example Corp,
 Inc.", "CountryCode": "US", "DistrictOrCounty": "King",
```

```
"FullName": "Saanvi Sarkar", "PhoneNumber": "+15555550100", "PostalCode": "98101",
 "StateOrRegion": "WA", "WebsiteUrl": "https://www.examplecorp.com"}'
```

Cette commande ne produit aucune sortie si elle réussit.

Mettez à jour le contact principal de n'importe quel contact Compte AWS au sein de votre organisation

Pour modifier vos coordonnées principales Compte AWS dans n'importe quel membre de votre organisation, suivez les étapes de la procédure suivante.

Exigences supplémentaires

Pour mettre à jour le contact principal avec la AWS Organizations console, vous devez définir certains paramètres préliminaires :

- Votre organisation doit activer toutes les fonctionnalités permettant de gérer les paramètres de vos comptes membres. Cela permet à l'administrateur de contrôler les comptes des membres. Ce paramètre est défini par défaut lorsque vous créez votre organisation. Si votre organisation est configurée pour la facturation consolidée uniquement et que vous souhaitez activer toutes les fonctionnalités, consultez la section Activation de toutes les fonctionnalités de votre organisation.
- Vous devez activer l'accès sécurisé pour le service de gestion des AWS comptes. Pour configurer cela, consultez la section Activation de l'accès sécurisé pour la gestion des AWS comptes.

AWS Management Console

Pour modifier le nom de votre contact principal pour n'importe quel Compte AWS membre de votre organisation

1. Connectez-vous à la AWS Organizationsconsole avec les informations d'identification du compte de gestion de l'organisation.
2. Dans Comptes AWS, sélectionnez le compte que vous souhaitez mettre à jour.
3. Choisissez Informations de contact, puis localisez le contact principal,
4. Tâche de sélection Modifier.
5. Modifiez les valeurs de l'un des champs disponibles.
6. Une fois que vous avez apporté toutes vos modifications, choisissez Mettre à jour.

AWS CLI & SDKs

Vous pouvez récupérer, mettre à jour ou supprimer les informations de contact principales à l'aide des AWS CLI commandes suivantes ou de leurs opérations équivalentes dans le AWS SDK :

- GetContactInformation
- PutContactInformation

> **Remarques**
>
> - Pour effectuer ces opérations à partir du compte de gestion ou d'un compte administrateur délégué d'une organisation sur les comptes des membres, vous devez activer l'accès sécurisé pour le service Account.
> - Vous ne pouvez pas accéder à un compte appartenant à une organisation différente de celle que vous utilisez pour appeler l'opération.

> **Autorisations minimales**
>
> Pour chaque opération, vous devez disposer de l'autorisation correspondant à cette opération :
>
> - `account:GetContactInformation`
> - `account:PutContactInformation`
>
> Si vous utilisez ces autorisations individuelles, vous pouvez autoriser certains utilisateurs à lire uniquement les informations de contact, tandis que d'autres peuvent lire et écrire.

Example

L'exemple suivant permet de récupérer les informations de contact principal actuelles pour le compte de membre spécifié dans une organisation. Les informations d'identification utilisées doivent provenir du compte de gestion de l'organisation ou du compte d'administrateur délégué de la gestion des comptes.

```
$ aws account get-contact-information --account-id 123456789012
```

```
{
    "ContactInformation": {
        "AddressLine1": "123 Any Street",
        "City": "Seattle",
        "CompanyName": "Example Corp, Inc.",
        "CountryCode": "US",
        "DistrictOrCounty": "King",
        "FullName": "Saanvi Sarkar",
        "PhoneNumber": "+15555550100",
        "PostalCode": "98101",
        "StateOrRegion": "WA",
        "WebsiteUrl": "https://www.examplecorp.com"
    }
}
```

Example

L'exemple suivant définit les informations de contact principales pour le compte de membre spécifié dans une organisation. Les informations d'identification utilisées doivent provenir du compte de gestion de l'organisation ou du compte d'administrateur délégué de la gestion des comptes.

```
$ aws account put-contact-information --account-id 123456789012 \
--contact-information '{"AddressLine1": "123 Any Street", "City": "Seattle",
 "CompanyName": "Example Corp, Inc.", "CountryCode": "US", "DistrictOrCounty":
 "King",
"FullName": "Saanvi Sarkar", "PhoneNumber": "+15555550100", "PostalCode": "98101",
 "StateOrRegion": "WA", "WebsiteUrl": "https://www.examplecorp.com"}'
```

Cette commande ne produit aucune sortie si elle réussit.

Mettre à jour les questions relatives aux défis de

Les questions de sécurité constituent une méthode de vérification utilisée précédemment pour vérifier une identité dans le cadre de scénarios de restauration de comptes. Ils sont moins sécurisés que les formes de vérification plus modernes, telles que l'authentification multifactorielle (MFA). Si des questions de sécurité sont actuellement actives sur votre compteCompte AWS, vous AWS Support pouvez les utiliser pour vous authentifier en tant que propriétaire du compte.

> **Important**
>
> À compter du 5 janvier 2024, les questions de sécurité ne AWS seront plus prises en charge pour les comptes qui ne les ont pas déjà activées et utilisées. Cela supprimera l'option permettant d'ajouter de nouvelles questions de sécurité sur la page Comptes duAWS Management Console. Si vous avez déjà défini des questions de sécurité ou si vous les avez déjà définies sur le compte de gestion de votre AWS organisation, vous pouvez continuer à les utiliser. Après le 6 janvier 2025, les questions relatives aux défis de sécurité ne AWS seront plus prises en charge pour tous les clients restants. Nous vous encourageons à ajouter le MFA à la place. Pour plus d'informations, consultez la section AWSLes comptes cessent d'utiliser les questions relatives aux défis de sécurité.

Pour modifier les questions de sécurité existantes et fournir les réponses, effectuez les étapes de la procédure suivante.

AWS Management Console

Pour modifier les questions relatives aux défis de sécurité pour votre Compte AWS

> **Autorisations minimales**
>
> Pour effectuer les étapes suivantes, vous devez au moins disposer des autorisations IAM suivantes :
>
> - `account:GetChallengeQuestions`(pour voir les questions relatives aux défis de sécurité)
> - `account:PutChallangeQuestions`(pour définir ou mettre à jour les questions relatives aux défis de sécurité)

1. Connectez-vous au en AWS Management Consoletant qu'utilisateur Utilisateur racine d'un compte AWS ou rôle IAM disposant des autorisations minimales.
2. Choisissez le nom de votre compte en haut à droite de la fenêtre, puis sélectionnez Compte.
3. Faites défiler la page jusqu'à la section Questions relatives aux défis de sécurité et choisissez Modifier.

> **Note**
>
> Si l'option Modifier n'apparaît pas, il est probable que vous ne soyez pas connecté en tant qu'utilisateur root de votre compte ou en tant que personne disposant des autorisations minimales spécifiées ci-dessus.

4. Modifiez les valeurs de l'un des champs disponibles. Vous pouvez sélectionner n'importe laquelle des questions proposées, puis saisir la réponse appropriée.
5. Après avoir effectué vos modifications, choisissez Mettre à jour.

AWS CLI & SDKs

Cette tâche n'est pas prise en charge dans l'AWS CLI ou par une opération d'API provenant de l'un des kits AWS SDK. Vous ne pouvez effectuer cette tâche qu'à l'aide de l'AWS Management Console.

Spécifiez ce Régions AWS que votre compte peut utiliser

An Région AWSest un emplacement physique dans le monde où nous avons plusieurs zones de disponibilité. Les zones de disponibilité se composent d'un ou de plusieurs centres de AWS données distincts, chacun doté d'une alimentation, d'un réseau et d'une connectivité redondants, hébergés dans des installations distinctes. Cela signifie que chacune Région AWS est physiquement isolée et indépendante des autres régions. Les régions fournissent une tolérance aux pannes, une stabilité et une résilience, et peuvent également réduire la latence. Pour une carte des régions disponibles et à venir, voir Régions et zones de disponibilité.

Les ressources que vous créez dans une région n'existent dans aucune autre région, sauf si vous utilisez explicitement une fonctionnalité de réplication proposée par un AWS service. Par exemple, Amazon S3 et Amazon EC2 prennent en charge la réplication entre régions. Certains services, tels que AWS Identity and Access Management (IAM), ne disposent pas de ressources régionales.

Votre compte détermine les régions qui vous sont disponibles.

- An Compte AWS fournit plusieurs régions afin que vous puissiez lancer AWS des ressources dans des emplacements qui répondent à vos besoins. Par exemple, vous souhaiterez peut-être lancer des instances Amazon EC2 en Europe pour vous rapprocher de vos clients européens ou pour répondre aux exigences légales.

- Un compte AWS GovCloud (US-West) donne accès à la région AWS GovCloud (US-Ouest) et à la région AWS GovCloud (US-Est). Pour plus d'informations, consultez AWS GovCloud (US).
- Un compte Amazon AWS (Chine) permet d'accéder uniquement aux régions de Pékin et de Ningxia. Pour plus d'informations, veuillez consulter Amazon Web Services en Chine.

Pour obtenir la liste des noms de régions et leurs codes correspondants, consultez la section Points de terminaison régionaux dans le Guide de référence AWS général. Pour obtenir la liste des AWS services pris en charge dans chaque région (sans les points de terminaison), consultez la liste des services AWS régionaux.

> **Important**
>
> AWS recommande d'utiliser des points de terminaison régionaux AWS Security Token Service (AWS STS) plutôt que des points de terminaison globaux afin de réduire la latence. Les jetons de session provenant des AWS STS points de terminaison régionaux sont valides dans toutes les AWS régions. Si vous utilisez des AWS STS points de terminaison régionaux, vous n'avez pas besoin d'apporter de modifications. Toutefois, les jetons de session provenant du point de AWS STS terminaison global (https://sts.amazonaws.com) ne sont valides Régions AWS que si vous les activez ou s'ils sont activés par défaut. Si vous avez l'intention d'activer une nouvelle région pour votre compte, vous pouvez soit utiliser des jetons de session provenant de AWS STS points de terminaison régionaux, soit activer le point de AWS STS terminaison mondial pour émettre des jetons de session valides pour tous Régions AWS. Les jetons de session valides dans toutes les régions sont plus importants. Si vous stockez des jetons de session, ces jetons plus importants peuvent affecter vos systèmes. Pour plus d'informations sur le fonctionnement des AWS STS terminaux avec AWS les régions, consultez la section Gestion AWS STS dans une AWS région.

Rubriques

Considérations à prendre en compte avant d'activer et de désactiver les régions

Avant d'activer ou de désactiver une région, il est important de prendre en compte les points suivants :

- Les régions introduites avant le 20 mars 2019 sont activées par défaut. AWS À l'origine, toutes les nouvelles régions étaient activées Régions AWS par défaut, ce qui signifie que vous pouvez commencer à créer et à gérer des ressources dans ces régions immédiatement. Vous ne pouvez pas activer ou désactiver une région activée par défaut. Aujourd'hui, lorsque vous AWS ajoutez une région, la nouvelle région est désactivée par défaut. Si vous souhaitez que vos utilisateurs puissent créer et gérer des ressources dans une nouvelle région, vous devez d'abord activer cette région. Les régions suivantes sont désactivées par défaut.

Nom	Code
Afrique (Le Cap)	`af-south-1`
Asie-Pacifique (Hong Kong)	`ap-east-1`
Asie-Pacifique (Hyderabad)	`ap-south-2`
Asie-Pacifique (Jakarta)	`ap-southeast-3`
Asie-Pacifique (Melbourne)	`ap-southeast-4`
Canada (Calgary)	`ca-west-1`
Europe (Milan)	`eu-south-1`
Europe (Espagne)	`eu-south-2`
Europe (Zurich)	`eu-central-2`
Israël (Tel Aviv)	`il-central-1`
Moyen-Orient (Bahreïn)	`me-south-1`
Moyen-Orient (EAU)	`me-central-1`

- Vous pouvez utiliser les autorisations IAM pour contrôler l'accès aux régions. AWS Identity and Access Management (IAM) inclut quatre autorisations qui vous permettent de contrôler quels utilisateurs peuvent activer, désactiver, obtenir et répertorier les régions. Pour plus d'informations, voir AWS: Autorise l'activation et la désactivation Régions AWS dans le guide de l'utilisateur IAM. Vous pouvez également utiliser la clé de `aws:RequestedRegion`condition pour contrôler l'accès Services AWS à un Région AWS.
- L'activation d'une région est gratuite — L'activation d'une région est gratuite. Seules les ressources que vous créez dans la nouvelle région vous sont facturées.
- La désactivation d'une région désactive l'accès IAM aux ressources de la région. Si vous désactivez une région qui contient encore des AWS ressources, telle que les instances Amazon Elastic Compute Cloud (Amazon EC2), vous perdez l'accès IAM aux ressources de cette région. Par exemple, vous ne pouvez pas utiliser le AWS Management Console pour afficher ou modifier la configuration d'une instance EC2 dans une région désactivée.
- Les frais pour les ressources actives continuent si vous désactivez une région — Si vous désactivez une région qui contient encore AWS des ressources, les frais pour ces ressources (le cas échéant) continuent de s'accumuler au taux standard. Par exemple, si vous désactivez une région qui contient des instances Amazon EC2, vous devrez encore payer ces frais pour ces instances même si celles-ci sont inaccessibles.
- La désactivation d'une région n'est pas toujours immédiatement visible : les services et les consoles peuvent être temporairement visibles après la désactivation d'une région. La désactivation d'une région peut prendre de quelques minutes à plusieurs heures pour prendre effet.
- L'activation d'une région prend de quelques minutes à plusieurs heures dans certains cas. Lorsque vous activez une région, vous effectuez AWS des actions pour préparer votre compte dans cette région, telles que la distribution de vos ressources IAM dans la région. Ce processus prend quelques minutes pour la plupart des comptes, mais peut parfois prendre plusieurs heures. Vous ne pouvez pas utiliser la région tant que ce processus n'est pas terminé.
- Organisations peuvent avoir 50 demandes optionnelles par région ouvertes à un moment donné au sein d'une AWS organisation. Le compte de gestion peut à tout moment avoir 50 demandes ouvertes en attente de traitement pour son organisation. Une demande équivaut à l'activation ou à la désactivation d'une région particulière pour un compte.
- Un seul compte peut avoir 6 demandes d'option de région en cours à tout moment. Une demande équivaut à l'activation ou à la désactivation d'une région en particulier pour un compte.
- EventBridge Intégration avec Amazon — Les clients peuvent s'abonner aux notifications de mise à jour de statut optées par région dans. EventBridge Une EventBridge notification sera créée pour chaque changement de statut, permettant aux clients d'automatiser les flux de travail.

- État d'option de région expressif — En raison de la nature asynchrone de l'activation/désactivation d'une région optionnelle, il existe quatre statuts potentiels pour une demande d'option de région :
  - `ENABLING`
  - `DISABLING`
  - `ENABLED`
  - `DISABLED`

  Vous ne pouvez pas annuler un opt-in ou un opt-out lorsqu'il est activé `ENABLING` ou non`DISABLING`. Dans le cas contraire, un `ConflictException` testament sera lancé. Une demande d'option de région terminée (activée/désactivée) dépend de la fourniture des principaux services sous-jacents. AWS Il se peut que certains AWS services ne soient pas immédiatement utilisables malgré leur statut`ENABLED`.
- Intégration complète avec AWS Organizations — Un compte de gestion peut modifier ou lire Region-Opt pour n'importe quel compte membre de cette AWS organisation. Un compte membre peut également lire/écrire l'état de sa région.

Activer ou désactiver une région pour les comptes autonomes

Pour mettre à jour les régions auxquelles vous Compte AWS avez accès, suivez les étapes de la procédure suivante. La AWS Management Console procédure ci-dessous ne fonctionne toujours que dans le contexte autonome. Vous pouvez utiliser le AWS Management Console pour afficher ou mettre à jour uniquement les régions disponibles dans le compte que vous avez utilisé pour appeler l'opération.

AWS Management Console

Pour activer ou désactiver une région pour un appareil autonome Compte AWS

> **Autorisations minimales**
>
> Pour effectuer les étapes de la procédure suivante, un utilisateur ou un rôle IAM doit disposer des autorisations suivantes :
>
> - `account:ListRegions`(nécessaire pour voir la liste des Régions AWS et savoir s'ils sont actuellement activés ou désactivés).
> - `account:EnableRegion`

- `account:DisableRegion`

1. Connectez-vous au en AWS Management Consoletant qu'utilisateur Utilisateur racine d'un compte AWS ou rôle IAM disposant des autorisations minimales.
2. Choisissez le nom de votre compte en haut à droite de la fenêtre, puis sélectionnez Compte.
3. Sur la page Compte, faites défiler la page vers le bas jusqu'à la section Régions AWS.

> **Note**
>
> Il se peut que vous soyez invité à approuver votre accès à ces informations. AWS envoie une demande à l'adresse e-mail associée au compte et au numéro de téléphone du contact principal. Choisissez le lien dans la demande pour l'ouvrir dans votre navigateur et approuvez l'accès.

4. À côté Région AWS de chaque option dans la colonne Action, choisissez Activer ou Désactiver, selon que vous souhaitez que les utilisateurs de votre compte puissent créer des ressources dans cette région et y accéder.
5. Si vous y êtes invité, confirmez votre choix.
6. Une fois que vous avez apporté toutes vos modifications, choisissez Mettre à jour.

AWS CLI & SDKs

Vous pouvez activer, désactiver, lire et répertorier le statut des options de région en utilisant les AWS CLI commandes suivantes ou leurs opérations équivalentes dans le AWS SDK :

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

> **Autorisations minimales**
>
> Pour effectuer les étapes suivantes, vous devez disposer de l'autorisation associée à cette opération :

- `account:EnableRegion`
- `account:DisableRegion`
- `account:GetRegionOptStatus`
- `account:ListRegions`

Si vous utilisez ces autorisations individuelles, vous pouvez autoriser certains utilisateurs à lire uniquement les informations relatives aux options de région, tandis que d'autres peuvent lire et écrire.

L'exemple suivant active une région pour le compte membre spécifié dans une organisation. Les informations d'identification utilisées doivent provenir du compte de gestion de l'organisation ou du compte d'administrateur délégué de la gestion des comptes.

Notez que vous pouvez également désactiver une région à l'aide de la même commande, puis en la `enable-region` remplaçant par`disable-region`.

```
aws account enable-region --region-name af-south-1
```

Cette commande ne produit aucune sortie si elle réussit.

L'opération est asynchrone. La commande suivante vous permettra de voir le dernier statut de la demande.

```
aws account get-region-opt-status --region-name af-south-1
  {
    "RegionName": "af-south-1",
    "RegionOptStatus": "ENABLING"
  }
```

Activer ou désactiver une région dans votre organisation

Pour mettre à jour les régions activées pour vos comptes membres AWS Organizations, suivez les étapes de la procédure suivante.

> **Note**
>
> Les politiques AWS Organizations `AWSOrganizationsReadOnlyAccess` gérées `AWSOrganizationsFullAccess` sont mises à jour pour autoriser l'accès aux API de gestion des AWS comptes afin que vous puissiez accéder aux données du compte depuis la AWS Organizations console. Pour consulter les politiques gérées mises à jour, voir Mises à jour des politiques AWS gérées par les Organizations.

> **Note**
>
> Avant de pouvoir effectuer ces opérations à partir du compte de gestion ou d'un compte d'administrateur délégué d'une organisation à utiliser avec les comptes des membres, vous devez :
>
> - Activez toutes les fonctionnalités de votre organisation pour gérer les paramètres de vos comptes membres. Cela permet à l'administrateur de contrôler les comptes des membres. Ce paramètre est défini par défaut lorsque vous créez votre organisation. Si votre organisation est configurée pour la facturation consolidée uniquement et que vous souhaitez activer toutes les fonctionnalités, consultez la section Activation de toutes les fonctionnalités de votre organisation.
> - Activez un accès sécurisé pour le service de gestion des AWS comptes. Pour configurer cela, voirPermettre un accès sécurisé pour la gestion des AWS comptes.

AWS Management Console

Pour activer ou désactiver une région dans votre organisation

1. Connectez-vous à la AWS Organizations console à l'aide des informations d'identification du compte de gestion de votre organisation.
2. Sur la Comptes AWSpage, sélectionnez le compte que vous souhaitez mettre à jour.
3. Choisissez l'onglet Paramètres du compte.
4. Sous Régions, sélectionnez la région que vous souhaitez activer ou désactiver.
5. Choisissez Actions, puis sélectionnez l'option Activer ou Désactiver.
6. Si vous avez choisi l'option Activer, passez en revue le texte affiché, puis choisissez Activer la région.

7. Si vous avez choisi l'option Désactiver, passez en revue le texte affiché, tapez désactiver pour confirmer, puis sélectionnez Désactiver la région.

AWS CLI & SDKs

Vous pouvez activer, désactiver, lire et répertorier le statut des options de région pour les comptes des membres de l'organisation à l'aide des AWS CLI commandes suivantes ou de leurs opérations équivalentes dans le AWS SDK :

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

> **Autorisations minimales**
>
> Pour effectuer les étapes suivantes, vous devez disposer de l'autorisation associée à cette opération :
>
> - `account:EnableRegion`
> - `account:DisableRegion`
> - `account:GetRegionOptStatus`
> - `account:ListRegions`

Si vous utilisez ces autorisations individuelles, vous pouvez autoriser certains utilisateurs à lire uniquement les informations relatives aux options de région, tandis que d'autres peuvent lire et écrire.

L'exemple suivant active une région pour le compte membre spécifié dans une organisation. Les informations d'identification utilisées doivent provenir du compte de gestion de l'organisation ou du compte d'administrateur délégué de la gestion des comptes.

Notez que vous pouvez également désactiver une région à l'aide de la même commande, puis en la `enable-region` remplaçant par`disable-region`.

```
aws account enable-region --account-id 123456789012 --region-name af-south-1
```

Cette commande ne produit aucune sortie si elle réussit.

> **Note**
>
> Une organisation ne peut recevoir que 20 demandes régionales à la fois. Sinon, vous recevrez un`TooManyRequestsException`.

L'opération est asynchrone. La commande suivante vous permettra de voir le dernier statut de la demande.

```
aws account get-region-opt-status --account-id 123456789012 --region-name af-south-1
  {
    "RegionName": "af-south-1",
    "RegionOptStatus": "ENABLING"
  }
```

Créez ou mettez à jour votre Compte AWS alias

Si vous souhaitez que l'URL de vos utilisateurs IAM contienne le nom de votre entreprise (ou un autre easy-to-remember identifiant) au lieu de l'Compte AWSID, vous pouvez créer un alias de compte.

Pour savoir comment créer ou mettre à jour un alias de compte, consultez la section Création, suppression et mise en liste d'un Compte AWS alias dans le guide de l'utilisateur IAM.

Facturation d'uneCompte AWS

Pour les procédures liées à la facturation et les tâches liées à votreCompte AWS, consultez les rubriques suivantes dans leAWS Billing and Cost ManagementGuide de l'utilisateur :

- Modification de la devise utilisée pour payer votre facture
- Mise à jour et suppression de numéros d'enregistrement fiscal
- Activation du paramètre des taxes de succession

Gérer des comptes en Inde

Si vous vous inscrivez à un nouveauCompte AWSet choisissez l'Inde comme adresse de contact, votre contrat d'utilisation est avecAmazon Internet Services Private Limited(AISPL), un localAWSseller in India.AISPL gère votre facturation, et le total de votre facture est indiqué en roupies indiennes (INR) au lieu de dollars américains (USD). Après avoir créé un compte avec AISPL, vous ne pouvez pas modifier le pays dans vos informations de contact.

Si vous avez unCompte AWSavec une adresse en Inde, votre compte est soit avecAWSou AISPL, selon la date à laquelle vous avez ouvert le compte. Pour savoir si votre compte est ouvert avecAWSou AISPL, voirDetermining which company your account is with. Si vous êtes un client AWS existant, vous pouvez continuer à utiliser votre Compte AWS. Vous pouvez également choisir d'avoir à la fois unCompte AWSet un compte AISPL, bien qu'ils ne puissent pas être consolidés dans le mêmeAWSorganisation. Pour plus d'informations sur la gestion d'unCompte AWS, voirGérez votreCompte AWS.

Si votre compte est auprès de l'AISPL, suivez les procédures décrites dans cette rubrique pour gérer votre compte. Cette rubrique explique comment créer un compte AISPL, modifier les informations relatives à votre compte AISPL et ajouter ou modifier votre numéro de compte permanent (PAN).

Dans le cadre de la vérification des cartes de paiement au cours de l'inscription, AISPL débite votre carte d'un montant de 2 INR. AISPL rembourse ce montant de 2 INR une fois la vérification terminée. Dans le cadre du processus de vérification, vous pouvez être redirigé vers votre banque.

Rubriques

Déterminez à quelle entreprise appartient votre compte

Les services AWS sont fournis par AWS et par AISPL. Utilisez cette procédure pour déterminer la société à laquelle est rattaché votre compte.

AWS Management Console

Pour déterminer la société à laquelle est rattaché votre compte

> **Autorisations minimales**
>
> Pour effectuer les étapes suivantes, vous devez disposer au moins des autorisations IAM suivantes :
>
> - Cette procédure ne nécessite aucune autorisation spéciale.

1. Ouvrez AWS Management Console à l'adresse AWS Management Console.
2. Dans le pied de page au bas de la page, consultez la notice de copyright. Si le copyright concerne Amazon Web Services, votre compte est rattaché à AWS. Si le copyright concerne Amazon Internet Services Private Ltd., votre compte est rattaché à AISPL.

AWS CLI & SDKs

Cette tâche n'est pas prise en charge dans leAWS CLIou par une opération d'API depuis l'un desAWSSDK. Vous pouvez effectuer cette tâche uniquement à l'aide duAWS Management Console.

Créez unCompte AWSavec AISPL

AISPL est un vendeur local deAWSen Inde. Utilisez la procédure suivante pour créer un compte AISPL si votre adresse de contact est en Inde.

AWS Management Console

Pour s'inscrire à un compte AISPL

> **Autorisations minimales**
>
> Pour effectuer les étapes suivantes, vous devez disposer au moins des autorisations IAM suivantes :

- Parce que cette opération se produit avant que vous n'ayez unCompte AWS, cette opération ne nécessite aucunAWSautorisations.

1. Ouvrez leAWS Management Console, puis choisissezConnectez-vous à la console.
2. Sur leConnectez-vouspage, entrez l'adresse e-mail que vous souhaitez utiliser.
3. Sous votre adresse e-mail, sélectionnez I am a new user, puis choisissez Sign in using our secure server.
4. Pour chacun des champs d'identification de connexion, entrez vos informations, puis choisissezCréer un compte.
5. Pour chacun des champs d'informations de contact, entrez vos informations.
6. Une fois que vous avez lu le contrat client, cochez la case des conditions générales, puis choisissez Créer un compte et continuer.
7. Sur la page Payment Information, entrez le moyen de paiement à utiliser.
8. SousInformations sur le PAN, choisissezNonsi vous n'avez pas de numéro de compte permanent (PAN) ou si vous souhaitez l'ajouter ultérieurement. Si vous avez un PAN et souhaitez l'ajouter maintenant, choisissezOui, et dans lePOÊLEEntrez votre PAN dans le champ.
9. Choisissez Vérifier la carte et continuer. Vous devez fournir votre valeur CVV dans le cadre du processus de vérification. AISPL débite votre carte d'un montant de 2 INR dans le cadre du processus de vérification. AISPL rembourse ce montant de 2 INR une fois la vérification terminée.
10. PourIndiquez un numéro de téléphone, entrez votre numéro de téléphone. Si vous avez une extension téléphonique, pourExt., saisissez le numéro de poste de votre téléphone.
11. Choisissez Appelez-moi maintenant. Après quelques instants, un code PIN à 4 chiffres s'affiche sur votre écran.
12. Acceptez l'appel automatisé d'AISPL. Sur le clavier de votre téléphone, saisissez le code PIN à quatre chiffres affiché à l'écran.
13. Une fois que l'appel automatisé vérifie votre numéro de contact, choisissez Continue to Select Your Support Plan.
14. Sur la page Support Plan, sélectionnez votre plan de support, puis choisissez Continuer. Une fois votre mode de paiement vérifié et votre compte activé, vous recevez un e-mail confirmant l'activation de votre compte.

AWS CLI & SDKs

Cette tâche n'est pas prise en charge dans leAWS CLIou par une opération d'API depuis l'un desAWSSDK. Vous pouvez effectuer cette tâche uniquement à l'aide duAWS Management Console.

Gérez votre compte AISPL

À l'exception des tâches suivantes, les procédures de gestion de votre compte sont les mêmes que pour les comptes créés en dehors de l'Inde. Consultez Gérez votreCompte AWS.

Utilisez leAWS Management Consolepour effectuer les tâches suivantes :

- Ajouter ou modifier un numéro de compte permanent (PAN)
- Modifier plusieurs numéros de compte permanents (PAN)
- Modifier plusieurs numéros de taxe sur les produits et services (TPS)
- Afficher une facture fiscale

Fermez un Compte AWS

Si vous n'avez plus besoin de votre Compte AWS, vous pouvez le fermer à tout moment en suivant les instructions de cette section. Après l'avoir fermé, vous pouvez le rouvrir dans les 90 jours suivant la date de fermeture du compte. La période entre le jour où vous avez fermé le compte et le moment où il est AWS définitivement fermé est appelée période postérieure à la fermeture.

Ce que vous devez savoir avant de fermer votre compte

Avant de fermer votre compte Compte AWS, vous devez tenir compte des points suivants :

- La fermeture de votre compte vous servira de notification de résiliation du contrat AWS client pour ce compte.
- Il n'est pas nécessaire de supprimer des ressources dans votre fichier Compte AWS avant de le fermer. Toutefois, nous vous recommandons de sauvegarder toutes les ressources ou données que vous souhaitez conserver. Pour obtenir des instructions sur la sauvegarde d'une ressource donnée, consultez la AWS documentation appropriée pour ce service.
- Vous pouvez rouvrir votre compte pendant la période suivant la fermeture. Les frais pour les services restés sur votre compte reprendront si vous le rouvrez. Vous restez également

responsable de toutes les factures impayées, des instances réservées et des Savings Plans impayés.

- Vous demeurez responsable de tous les frais impayés et des charges relatifs aux services consommés avant la fermeture du compte. Vous recevrez une AWS facture le mois suivant la fermeture de votre compte. Par exemple, si vous avez fermé votre compte le 15 janvier, vous recevrez une facture début février pour l'utilisation effectuée entre le 1er et le 15 janvier. Vous continuerez à recevoir des factures pour les instances réservées et les Savings Plans après la fermeture de votre compte jusqu'à leur expiration.
- Vous ne pourrez plus accéder aux AWS services qui étaient auparavant disponibles dans votre compte. Cependant, vous pouvez vous connecter et accéder à un compte fermé Compte AWS pendant la période suivant la fermeture uniquement pour consulter les informations de facturation passées, accéder aux paramètres du compte ou contacter. AWS Support
- Vous ne pouvez pas utiliser la même adresse e-mail que celle que vous avez enregistrée Compte AWS au moment de sa fermeture comme adresse e-mail principale d'une autre personne Compte AWS. Si vous souhaitez utiliser la même adresse e-mail pour une autre Compte AWS, nous vous recommandons de la mettre à jour avant la fermeture. Consultez Mettre à jour le Compte AWS nom, l'adresse e-mail ou le mot de passe de l'utilisateur root les instructions relatives à la mise à jour de votre adresse e-mail.
- Si vous avez activé l'authentification multifactorielle (MFA) sur Compte AWS votre utilisateur root ou configuré un dispositif MFA sur un utilisateur IAM, l'authentification MFA n'est pas supprimée automatiquement lorsque vous fermez le compte. Si vous choisissez de laisser le MFA activé pendant la période de 90 jours suivant la fermeture, maintenez le dispositif MFA actif jusqu'à l'expiration de la période postérieure à la fermeture au cas où vous auriez besoin d'accéder au compte pendant cette période. Notez que les dispositifs matériels à jetons TOTP ne peuvent pas être associés à un autre utilisateur après la fermeture définitive de votre compte. Si vous souhaitez utiliser le jeton TOTP matériel avec un autre utilisateur ultérieurement, vous avez la possibilité de désactiver le dispositif MFA matériel avant de fermer le compte. Les dispositifs MFA pour les utilisateurs IAM doivent être supprimés par l'administrateur du compte.

Considérations supplémentaires concernant les comptes des membres

- Lorsque vous fermez un compte membre, ce compte n'est retiré de l'organisation qu'après la fin de la période postérieure à la fermeture. Pendant la période de post-clôture, un compte de membre fermé est toujours comptabilisé dans votre quota de comptes au sein de l'organisation. Pour éviter que le compte ne soit pris en compte dans le quota, voir Supprimer un compte membre de votre organisation avant de la fermer.

- Vous ne pouvez clôturer que 10 % des comptes membres au cours d'une période continue de 30 jours. Ce quota n'est pas lié au mois civil, mais commence lorsque vous fermez un compte. Dans les 30 jours suivant la fermeture initiale du compte, vous ne pouvez pas dépasser la limite de 10 %. La clôture minimale de compte est de 10 et la fermeture maximale de 1 000 comptes, même si 10 % des comptes dépassent 1 000. Pour plus d'informations sur les quotas des Organisations, consultez la section Quotas pour AWS Organizations.
- Si vous utilisez AWS Control Tower, vous devez annuler la gestion du compte membre avant de tenter de le fermer. Veuillez consulter la section Supprimer la gestion d'un compte membre dans le Guide de l'utilisateur d' AWS Control Tower.

Considérations spécifiques au service

- AWS Marketplace les abonnements ne sont pas automatiquement annulés à la fermeture du compte. Si vous avez des abonnements, mettez d'abord fin à toutes les instances de votre logiciel incluses dans les abonnements. Accédez ensuite à la page Gérer les abonnements de la AWS Marketplace console et annulez vos abonnements.
- Les domaines enregistrés avec Route 53 ne sont pas supprimés automatiquement. Avant de fermer votre compte Compte AWS, quatre options s'offrent à vous :
  - Vous pouvez désactiver le renouvellement automatique et les domaines sont automatiquement supprimés à l'expiration de la période d'enregistrement. Pour plus d'informations, veuillez consulter Activation ou désactivation du renouvellement automatique pour un domaine dans le Guide du développeur Amazon Route 53.
  - Vous pouvez transférer les domaines vers un autre Compte AWS. Pour plus d'informations, consultez Transfert d'un domaine vers un autre Compte AWS.
  - Vous pouvez transférer les domaines vers un autre bureau d'enregistrement de domaine. Pour plus d'informations, voir Transfert d'un domaine de Route 53 vers un autre bureau d'enregistrement.
  - Si vous avez déjà fermé votre compte, vous pouvez ouvrir un dossier AWS Support pour obtenir de l'aide pour transférer le domaine.
- AWS CloudTrail est un service de sécurité fondamental. Cela signifie que les parcours créés par les utilisateurs continuent d'exister et de proposer des événements même après la fermeture d'un AWS compte, sauf si un utilisateur supprime explicitement les sentiers de son AWS compte avant de le fermer. Ce comportement s’applique également aux journaux de suivi d’organisation crées par le compte de gestion ou par l’administrateur délégué, ainsi qu’aux journaux de suivi d’organisation multi-Régions qui sont ensuite créés dans les comptes des membres de

l'organisation. Pour plus d'informations, consultez la section Fermeture du AWS compte et itinéraires dans le guide de CloudTrail l'utilisateur.

Comment fermer votre compte

Vous pouvez fermer votre compte Compte AWS en procédant comme suit. Notez que des instructions différentes sont fournies dans chaque onglet en fonction du type de compte [autonome, membre, direction et AWS GovCloud (US)] que vous souhaitez fermer.

Si vous rencontrez des problèmes lors de la fermeture de votre compte, consultezRésolution des problèmes liés à Compte AWS la fermeture.

Standalone account

Un compte autonome est un compte géré individuellement qui ne fait pas partie de AWS Organizations.

Pour fermer un compte autonome depuis la page Comptes

1. Connectez-vous en AWS Management Console tant qu'utilisateur root dans le fichier Compte AWS que vous souhaitez fermer. Vous ne pouvez pas fermer un compte lorsque vous êtes connecté en tant qu'utilisateur ou en tant que rôle IAM.
2. Dans la barre de navigation située dans le coin supérieur droit, choisissez le nom ou le numéro de votre compte, puis sélectionnez Compte.
3. Sur la page Compte, cliquez sur le bouton Fermer le compte.
4. Entrez votre identifiant de compte (affiché en haut de la boîte de dialogue de fermeture) pour confirmer que vous avez lu et compris le processus de fermeture du compte.
5. Cliquez sur le bouton Fermer le compte pour lancer le processus de fermeture du compte.
6. Dans quelques minutes, vous devriez recevoir un e-mail de confirmation indiquant que votre compte a été fermé.

> **Note**
>
> Cette tâche n'est pas prise en charge dans AWS CLI ou par une opération d'API provenant de l'un des AWS SDK. Vous ne pouvez effectuer cette tâche qu'à l'aide du AWS Management Console.

Member account

Un compte de membre est un compte Compte AWS qui fait partie de AWS Organizations.

Pour fermer un compte membre depuis la AWS Organizations console

1. Connectez-vous à la console AWS Organizations.
2. Sur la page Comptes AWS, trouvez et choisissez le nom du compte membre que vous souhaitez clôturer. Vous pouvez naviguer dans la hiérarchie des unités organisationnelles (OU), consulter une liste plate de comptes sans la structure des OU.
3. Choisissez Close (Clôturer) en regard du nom du compte en haut de la page. Organisations en mode facturation consolidée ne pourront pas voir le bouton Fermer dans la console. Pour fermer un compte en mode de facturation consolidée, vous devez suivre les étapes indiquées dans l'onglet Compte autonome.
4. Lisez les instructions de fermeture de compte et assurez-vous de bien les comprendre.
5. Entrez l'identifiant du compte du membre, puis choisissez Fermer le compte pour lancer le processus de fermeture du compte.

Pour fermer un compte membre depuis la page Comptes

Vous pouvez éventuellement fermer un compte AWS membre directement depuis la page Compte du AWS Management Console. Pour step-by-step obtenir des conseils, suivez les instructions de l'onglet Compte autonome.

Pour fermer un compte membre à l'aide de kits AWS CLI de développement logiciel

Pour savoir comment fermer un compte membre à l'aide des SDK AWS CLI et, consultez la section Fermeture d'un compte membre dans votre organisation dans le Guide de l'AWS Organizations utilisateur.

Management account

Un compte de gestion est un compte Compte AWS qui agit en tant que compte parent ou root pour AWS Organizations.

> **Note**
>
> Vous ne pouvez pas fermer un compte de gestion directement depuis la AWS Organizations console.

Pour fermer un compte de gestion depuis la page Comptes

1. Connectez-vous en AWS Management Console tant qu'utilisateur root pour le compte de gestion que vous souhaitez fermer. Vous ne pouvez pas fermer un compte lorsque vous êtes connecté en tant qu'utilisateur ou en tant que rôle IAM.
2. Vérifiez qu'il ne reste aucun compte de membre actif dans votre organisation. Pour ce faire, accédez à la AWS Organizations console et assurez-vous que tous les comptes des membres apparaissent à `Suspended` côté de leur nom de compte. Si vous avez un compte membre toujours actif, vous devrez suivre les instructions de fermeture de compte fournies dans l'onglet Compte membre avant de passer à l'étape suivante.
3. Dans la barre de navigation située dans le coin supérieur droit, choisissez le nom ou le numéro de votre compte, puis sélectionnez Compte.
4. Sur la page Compte, cliquez sur le bouton Fermer le compte.
5. Entrez votre identifiant de compte (affiché en haut de la boîte de dialogue de fermeture) pour confirmer que vous avez lu et compris le processus de fermeture du compte.
6. Cliquez sur le bouton Fermer le compte pour lancer le processus de fermeture du compte.
7. Dans quelques minutes, vous devriez recevoir un e-mail de confirmation indiquant que votre compte a été fermé.

> **Note**
>
> Cette tâche n'est pas prise en charge dans AWS CLI ou par une opération d'API provenant de l'un des AWS SDK. Vous ne pouvez effectuer cette tâche qu'à l'aide du AWS Management Console.

AWS GovCloud (US) account

Un AWS GovCloud (US) compte est toujours lié à une norme unique à Compte AWS des fins de facturation et de paiement.

Pour fermer un AWS GovCloud (US) compte

Si vous avez un Compte AWS compte lié à un AWS GovCloud (US) compte, vous devez fermer le compte standard avant de fermer le AWS GovCloud (US) compte. Pour plus de détails, notamment sur la manière de sauvegarder les données et d'éviter des AWS GovCloud (US) frais

imprévus, consultez la section Fermeture d'un AWS GovCloud (US) compte dans le guide de l' AWS GovCloud (US) utilisateur.

À quoi s'attendre après la fermeture de votre compte

Immédiatement après la fermeture de votre compte, les événements suivants se produiront :

- Vous recevrez un e-mail confirmant la fermeture du compte à l'adresse e-mail de l'utilisateur root. Si vous ne recevez pas cet e-mail dans les heures qui suivent, consultezRésolution des problèmes liés à Compte AWS la fermeture.
- Tout compte de membre que vous fermez affichera une `SUSPENDED` étiquette à côté de son nom dans la AWS Organizations console.
- Si vous avez autorisé l'accès aux services de votre compte Compte AWS à d'autres comptes, toutes les demandes d'accès effectuées à partir de ces comptes devraient échouer après la fermeture du compte. Si vous rouvrez votre compte Compte AWS, d'autres Comptes AWS personnes pourront à nouveau accéder aux AWS services et aux ressources de votre compte si vous leur avez accordé les autorisations nécessaires.

Période postérieure à la fermeture

La période postérieure à la fermeture fait référence à la période entre le jour où vous avez fermé votre compte et le moment où vous le fermez AWS Compte AWS définitivement. La période postérieure à la fermeture est de 90 jours. Pendant la période suivant la fermeture, vous ne pourrez accéder à votre contenu et à vos AWS services qu'en rouvrant votre compte. Après la période post-fermeture, ferme AWS définitivement le vôtre Compte AWS et vous ne pouvez plus le rouvrir. AWS supprimera également tout contenu et toutes les ressources de votre compte. Après la fermeture définitive d'un compte, son Compte AWS identifiant ne peut jamais être réutilisé.

Réouverture de votre Compte AWS

Votre compte sera définitivement fermé dans 90 jours, après quoi vous ne pourrez plus le rouvrir et vous AWS supprimerez le contenu restant sur votre compte. Pour rouvrir votre compte avant sa fermeture définitive, (1) vous devez nous contacter AWS Supportdès que possible, et (2) nous devons recevoir le paiement intégral de tout solde impayé, y compris en fournissant les informations requises telles que spécifiées sur la facture, dans les 60 jours suivant la date de fermeture du compte.

> **Note**
>
> Les frais pour les services restés sur votre compte reprendront si vous le rouvrez.

Utilisation de la gestion des AWS comptes dans votre organisation

AWS Organizationsest un AWS service que vous pouvez utiliser pour gérer votre Comptes AWS groupe. Cela fournit des fonctionnalités telles que la facturation consolidée, où toutes les factures de vos comptes sont regroupées et gérées par un seul payeur. Vous pouvez également gérer de manière centralisée la sécurité de votre organisation à l'aide de contrôles basés sur des politiques. Pour plus d'informations sur AWS Organizations, consultez le AWS OrganizationsGuide de l'utilisateur .

Accès sécurisé

Lorsque vous gérez AWS Organizations vos comptes en tant que groupe, la plupart des tâches administratives de l'organisation peuvent être effectuées uniquement par le compte de gestion de l'organisation. Par défaut, cela inclut uniquement les opérations liées à la gestion de l'organisation elle-même. Vous pouvez étendre cette fonctionnalité supplémentaire à d'autres AWS services en activant un accès sécurisé entre les organisations et ce service. L'accès sécurisé autorise le AWS service spécifié à accéder aux informations relatives à l'organisation et aux comptes qu'elle contient. Lorsque vous activez un accès sécurisé pour la gestion des comptes, le service de gestion des comptes autorise les organisations et leurs comptes de gestion à accéder aux métadonnées, telles que les informations de contact principales ou secondaires, pour tous les comptes membres de l'organisation.

Pour plus d'informations, veuillez consulter Permettre un accès sécurisé pour la gestion des AWS comptes.

Administrateur délégué

Après avoir activé l'accès sécurisé, vous pouvez également choisir de désigner l'un de vos comptes de membre comme compte administrateur délégué pour AWS la gestion des comptes. Cela permet au compte administrateur délégué d'effectuer les mêmes tâches de gestion des métadonnées de gestion des comptes pour les comptes des membres de votre organisation que seul le compte de gestion pouvait effectuer auparavant. Le compte administrateur délégué peut accéder uniquement aux tâches de gestion du service de gestion des comptes. Le compte administrateur délégué ne dispose pas de tous les accès administratifs à l'organisation dont dispose le compte de gestion.

Pour plus d'informations, veuillez consulter Activation d'un compte administrateur délégué pourAWSGestion de compte.

Politiques de contrôle des services

Lorsque vous Compte AWS faites partie d'une organisation gérée parAWS Organizations, l'administrateur de l'organisation peut appliquer des politiques de contrôle des services (SCP) qui peuvent limiter les actions des responsables des comptes membres. Un SCP n'accorde jamais d'autorisations ; il s'agit plutôt d'un filtre qui limite les autorisations pouvant être utilisées par le compte du membre. Un utilisateur ou un rôle (un principal) d'un compte de membre ne peut effectuer que les opérations qui se situent à l'intersection de ce qui est autorisé par les SCP qui s'appliquent au compte et des politiques d'autorisation IAM associées au principal. Par exemple, vous pouvez utiliser des SCP pour empêcher les principaux utilisateurs d'un compte de modifier les contacts secondaires de leur propre compte.

Par exemple, les SCP qui s'appliquent àComptes AWS, voirRestriction de l'accès avecAWS Organizationsstratégies de contrôle des services.

Permettre un accès sécurisé pour la gestion des AWS comptes

L'activation d'un accès sécurisé pour la gestion des AWS comptes permet à l'administrateur du compte de gestion de modifier les informations et les métadonnées (par exemple, les coordonnées principales ou secondaires) spécifiques à chaque compte de membre dansAWS Organizations. Pour plus d'informations, consultez la section Gestion des AWS comptes et AWS Organizations le Guide de AWS Organizations l'utilisateur. Pour des informations générales sur le fonctionnement de l'accès sécurisé, consultez la section Utilisation AWS Organizations avec d'autres AWS services.

Une fois l'accès sécurisé activé, vous pouvez utiliser le `accountID` paramètre dans les opérations de l'API de gestion de compte qui le prennent en charge. Vous ne pouvez utiliser ce paramètre correctement que si vous appelez l'opération à l'aide des informations d'identification du compte de gestion ou du compte administrateur délégué de votre organisation si vous en activez un. Pour plus d'informations, veuillez consulter Activation d'un compte administrateur délégué pourAWSGestion de compte.

Utilisez la procédure suivante pour activer un accès sécurisé pour la gestion des comptes dans votre organisation.

> **Autorisations minimales**
>
> Pour effectuer ces tâches, vous devez remplir les conditions suivantes :

- Vous ne pouvez effectuer cette opération qu'à partir du compte de gestion de l'organisation.
- Toutes les fonctions doivent être activées pour votre organisation.

AWS Management Console

Pour activer un accès sécurisé pour la gestion des AWS comptes

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Choisissez Services dans le volet de navigation.
3. Choisissez Gestion du AWS compte dans la liste des services.
4. Choisissez Enable trusted access (Activer l'accès approuvé).
5. Dans la boîte de dialogue Activer l'accès sécurisé pour la gestion des AWS comptes, tapez activer pour le confirmer, puis choisissez Activer l'accès sécurisé.

AWS CLI & SDKs

Pour activer un accès sécurisé pour la gestion des AWS comptes

Après avoir exécuté la commande suivante, vous pouvez utiliser les informations d'identification du compte de gestion de l'organisation pour appeler les opérations de l'API de gestion des comptes qui utilisent le `--accountId` paramètre pour référencer les comptes des membres d'une organisation.

- AWS CLI: enable-aws-service-access

  L'exemple suivant active un accès sécurisé pour la gestion des AWS comptes au sein de l'organisation du compte appelant.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal account.amazonaws.com
  ```

  Cette commande ne produit aucune sortie si elle réussit.

Activation d'un compte administrateur délégué pourAWSGestion de compte

Un compte administrateur délégué peut appeler leAWSOpérations d'une API de gestion de compte pour les autres comptes membres de l'organisation. Pour désigner un compte membre de votre organisation en tant que compte administrateur délégué, procédez comme suit.

Autorisations minimales

Pour effectuer ces tâches, vous devez remplir les conditions suivantes :

- Vous ne pouvez effectuer cette opération qu'à partir du compte de gestion de l'organisation.
- Toutes les fonctions doivent être activées pour votre organisation.
- Vous devez avoiraccès sécurisé activé pour la gestion des comptes dans votre organisation.

Une fois que vous avez spécifié un compte d'administrateur délégué pour votre organisation, les utilisateurs et les rôles de ce compte peuvent appeler leAWS CLIetAWSOpérations SDK dans le`account`espace de noms pouvant fonctionner en mode Organizations en prenant en charge une option`AccountId` Paramètre .

AWS Management Console

Cette tâche n'est pas prise en charge dans leAWSConsole de gestion de compte. Vous ne pouvez effectuer cette tâche qu'à l'aide duAWS CLIou une opération API à partir de l'un desAWSKits SDK.

AWS CLI & SDKs

Pour enregistrer un compte administrateur délégué pour le service de gestion de compte

Vous pouvez utiliser les commandes suivantes pour activer un administrateur délégué pour le service de gestion de compte.

Vous devez spécifier le principal de service suivant :

```
account.amazonaws.com
```

- AWS CLI :Administrateur-Délégat-Registre

  L'exemple suivant montre comment enregistrer un compte membre de l'organisation en tant qu'administrateur délégué pour le service Gestion des comptes.

  ```
  $ aws organizations register-delegated-administrator \
      --account-id 123456789012 \
      --service-principal account.amazonaws.com
  ```

  Cette commande ne produit aucune sortie si elle réussit.

  Après avoir exécuté cette commande, vous pouvez utiliser les informations d'identification du compte 123456789012 pour appeler Account ManagementAWS CLIet les opérations de l'API SDK qui utilisent le`--account-id`pour référencer les comptes membres dans une organisation.

Restriction de l'accès avecAWS Organizationsstratégies de contrôle des services

Cette rubrique présente des exemples qui montrent comment vous pouvez utiliser des stratégies de contrôle des services (SCP) pour restreindre les actions des utilisateurs et des rôles dans les comptes de votre organisation. Pour de plus amples informations sur les stratégies de contrôle des services, veuillez consulter les rubriques suivantes dans leAWS OrganizationsGuide de l'utilisateur :

- Création de SCP
- Associer des SCP aux unités opérationnelles et aux comptes
- Stratégies pour les SCP
- Syntaxe de la stratégie SCP

Example Exemple 1 : Empêcher les comptes de modifier leurs propres contacts alternatifs

L'exemple suivant ne permet pas de`PutAlternateContact`et`DeleteAlternateContact`les opérations d'API qui peuvent être appelées par n'importe quel compte membre dansmode compte autonome. Cela empêche tout mandant des comptes concernés de modifier ses propres contacts alternatifs.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Deny",
            "Action": [
                "account:PutAlternateContact",
                "account:DeleteAlternateContact"
            ],
            "Resource": [ "arn:aws:account::*:account" ]
        }
    ]
}
```

Example Exemple 2 : Empêcher tout compte de membre de modifier des contacts alternatifs pour tout autre compte membre de l'organisation

L'exemple suivant permet de généraliser le`Resource`à « * », ce qui signifie qu'il s'applique à la foisdemandes en mode autonome et demandes en mode organisations. Cela signifie que même le compte administrateur délégué pour la gestion des comptes, si le SCP s'applique à lui, ne peut pas changer de contact alternatif pour n'importe quel compte de l'organisation.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Deny",
            "Action": [
                "account:PutAlternateContact",
                "account:DeleteAlternateContact"
            ],
            "Resource": [ "*" ]
        }
    ]
}
```

Example Exemple 3 : Empêcher un compte membre d'une unité d'organisation de modifier ses propres contacts de remplacement

L'exemple de SCP suivant inclut une condition qui compare le chemin d'organisation du compte à une liste de deux unités d'organisation. Cela a pour effet d'empêcher un mandant de n'importe quel compte dans les unités d'organisation spécifiées de modifier ses propres contacts alternatifs.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Deny",
            "Action": "account:PutAlternateContact",
            "Resource": [
                "arn:aws:account::*:account"
            ],
            "Condition": {
                "ForAnyValue:StringLike": {
                    "account:AccountResourceOrgPath": [
                        "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/",
                        "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h222/"
                    ]
                }
            }
    ]
}
```

Sécurité dansAWSGestion de compte

Chez AWS, la sécurité dans le cloud est notre priorité numéro 1. En tant que client AWS, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des organisations les plus pointilleuses en termes de sécurité.

La sécurité est une responsabilité partagée entre AWS et vous. Le modèle de responsabilité partagéede décrit ceci comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est responsable de la protection de l'infrastructure qui exécute des services AWS dans le cloud AWS Cloud. AWS vous fournit également les services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des AWS programmes de conformité. Pour de plus d'informations sur les programmes de conformité qui s'appliquent à Gestion de compte, veuillez consulterServices AWSdans la portée par programme de conformité.
- Sécurité dans le cloud : votre responsabilité est déterminée par le service AWS que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre entreprise,et la législation et la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lorsque vous utilisezAWSGestion de compte. Elle vous montre comment configurer Gestion de compte pour atteindre vos objectifs en matière de sécurité et de conformité. Vous pouvez également apprendre à utiliser d'autresAWSServices qui vous aident à surveiller et sécuriser vos ressources de Gestion de votre compte.

Rubriques

Protection des données dans la gestion des AWS comptes

Le modèle de responsabilité AWS partagée Le modèle s'applique à la protection des données dans la gestion des AWS comptes. Comme décrit dans ce modèle, AWS est responsable de la protection de l'infrastructure globale sur laquelle l'ensemble du AWS Cloud s'exécute. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité pour les Services AWS que vous utilisez. Pour en savoir plus sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWSet RGPD (Règlement général sur la protection des données) sur le AWSBlog de sécurité.

À des fins de protection des données, nous vous recommandons de protéger les informations d'identification Compte AWS et de configurer les comptes utilisateur individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez les certificats SSL/TLS pour communiquer avec les ressources AWS. Nous exigeons TLS 1.2 et nous recommandons TLS 1.3.
- Configurez une API (Interface de programmation) et le journal de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de chiffrement AWS, ainsi que tous les contrôles de sécurité par défaut au sein des Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés FIPS (Federal Information Processing Standard) 140-2 lorsque vous accédez à AWS via une CLI (Interface de ligne de commande) ou une API (Interface de programmation), utilisez un point de terminaison FIPS (Federal Information Processing Standard). Pour en savoir plus sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels

que le champ Name (Nom). Cela inclut lorsque vous travaillez avec Account Management ou autre à Services AWS l'aide de la console, de l'API ou AWS des SDK. AWS CLI Toutes les données que vous saisissez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

AWS PrivateLinkpourAWSGestion de compte

Si vous utilisez Amazon Virtual Private Cloud (Amazon VPC) pour héberger votreAWS, vous pouvez accéder auAWSService de gestion de compte depuis le VPC sans avoir à traverser l'Internet public.

Amazon VPC vous permet de lancerAWSdans un réseau virtuel personnalisé. Vous pouvez utiliser un VPC pour contrôler vos paramètres réseau, tels que la plage d'adresses IP, les sous-réseaux, les tables de routage et les passerelles réseau. Pour plus d'informations sur le VPCs, consultez leAmazon VPC User Guide.

Pour connecter votre Amazon VPC à Account Management, vous devez d'abord définir unPoint de terminaison d'un VPC d'interface, qui vous permet de connecter votre VPC à d'autresAWSServices . Le point de terminaison assure une connectivité évolutive et fiable, sans qu'une passerelle Internet, une instance NAT (Network Address Translation) ou une connexion VPN ne soit nécessaire. Pour de plus amples informations, consultez Points de terminaison VPC (AWS PrivateLink) dans le Guide de l'utilisateur Amazon VPC.

Création du point de terminaison

Vous pouvez créer uneAWSPoint de terminaison Account Management dans votre VPC en utilisant leAWS Management Console, leAWS Command Line Interface(AWS CLI), unAWSkit SDK, leAWSAPI de gestion de compte, ouAWS CloudFormation.

Pour plus d'informations sur la création et la configuration d'un point de terminaison à l'aide de la console Amazon VPC ou de la AWS CLI, consultez la section Création d'un point de terminaison d'interface dans le Guide de l'utilisateur Amazon VPC.

> **Note**
>
> Lorsque vous créez un point de terminaison, spécifiez que Account Management est le service auquel vous voulez que votre VPC se connecte, au format suivant :

```
com.amazonaws.us-east-1.account
```

Vous devez utiliser la chaîne exactement comme indiqué, en spécifiant laus-east-1Région . En tant que service mondial, la gestion des comptes est hébergée uniquement dans celui-ciAWSRégion .

Pour plus d'informations sur la création et la configuration d'un point de terminaison avec AWS CloudFormation, consultez la ressource AWS::EC2::VPCEndpoint dans le Guide de l'utilisateur AWS CloudFormation.

Stratégies de point de terminaison Amazon VPC

Vous pouvez contrôler les actions qui peuvent être effectuées via ce point de terminaison de service en attachant une stratégie de point de terminaison lorsque vous créez le point de terminaison Amazon VPC. Vous pouvez créer des règles IAM complexes en attachant plusieurs stratégies de point de terminaison. Pour plus d'informations, consultez :

- Stratégies de point de terminaison Amazon Virtual Private Cloud pour Gestion de compte
- Contrôle de l'accès aux services avec les points de terminaison d'un VPCdans leAWS PrivateLinkGuide.

Stratégies de point de terminaison Amazon Virtual Private Cloud pour Gestion de compte

Vous pouvez créer une stratégie de point de terminaison Amazon VPC pour Gestion de compte dans laquelle vous spécifiez les éléments suivants :

- Le principal qui peut exécuter des actions.
- Les actions que les directeurs peuvent effectuer.
- La ressource sur laquelle les actions peuvent être effectuées.

L'exemple suivant montre une stratégie de point de terminaison Amazon VPC qui permet à un utilisateur IAM nommé Alice dans le compte 123456789012 de récupérer et de modifier les autres

informations de contact pour n'importe quelCompte AWS, mais refuse à tous les utilisateurs IAM l'autorisation de supprimer toute autre information de contact sur n'importe quel compte.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "account:GetAlternateContact",
                "account:PutAlternateContact"
            ],
            "Resource": "arn:aws::iam:*:account,
            "Effect": "Allow",
            "Principal": {
              "AWS": "arn:aws::iam:123456789012:user/Alice"
            }
        },
        {
            "Action": "account:DeleteAlternateContact",
            "Resource": "*",
            "Effect": "Deny",
            "Principal": "arn:aws::iam:*:root"
        }
    ]
}
```

Si vous voulez accorder un accès à des comptes faisant partie d'unAWSOrganisation vers un principal qui se trouve dans l'un des comptes membres de l'organisation, puis le`Resource`doit utiliser le format suivant :

```
arn:aws:account::{ManagementAccountId}:account/o-{OrganizationId}/{AccountId}
```

Pour plus d'informations sur la création des stratégies de point de terminaison, consultezContrôle de l'accès aux services avec les points de terminaison d'un VPCdans leAWS PrivateLinkGuide.

Identity and Access Management pour la gestion des AWS comptes

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs

IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources de gestion des comptes. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans la gestion des comptes.

Utilisateur du service : si vous utilisez le service de gestion des comptes pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités de gestion de compte pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne parvenez pas à accéder à une fonctionnalité de la gestion des comptes, consultezRésolution des problèmes d'identité et d'accès à la gestion des AWS comptes.

Administrateur du service — Si vous êtes responsable des ressources de gestion des comptes au sein de votre entreprise, vous avez probablement un accès complet à la gestion des comptes. C'est à vous de déterminer les fonctionnalités et les ressources de gestion des comptes auxquelles les utilisateurs du service doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d’IAM. Pour en savoir plus sur la façon dont votre entreprise peut utiliser IAM avec la gestion des comptes, consultezComment fonctionne la gestion des AWS comptes avec IAM.

Administrateur IAM : si vous êtes administrateur IAM, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à la gestion des comptes. Pour

consulter des exemples de politiques basées sur l'identité de gestion des comptes que vous pouvez utiliser dans IAM, consultez. Exemples de politiques basées sur l'identité pour AWS la gestion des comptes

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section Signature des demandes AWS d'API dans le guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

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

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus

d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent

le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur IAM.

- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.
  - Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
  - Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations,

consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principals (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAF Pour en savoir plus sur les listes de contrôle d'accès, consultez Vue d'ensemble des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans. AWS Organizations AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment fonctionne la gestion des AWS comptes avec IAM

Avant d'utiliser IAM pour gérer l'accès à la gestion des comptes, découvrez quelles fonctionnalités IAM peuvent être utilisées avec la gestion des comptes.

Fonctionnalités IAM que vous pouvez utiliser avec la gestion des AWS comptes

Fonction IAM	Assistance à la gestion des comptes
Politiques basées sur l’identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition d’une politique	Oui
ACL	Non
ABAC (étiquettes dans les politiques)	Oui
Informations d’identification temporaires	Oui
Autorisations de principal	Oui
Fonctions du service	Non
Rôles liés à un service	Non

Pour obtenir une vue d'ensemble de la façon dont la gestion des comptes et les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez la section AWS Services compatibles avec IAM dans le Guide de l'utilisateur IAM.

Politiques basées sur l'identité pour la gestion des comptes

Prend en charge les politiques basées sur l’identité	Oui

Les politiques basées sur l’identité sont des documents de politique d’autorisations JSON que vous pouvez attacher à une identité telle qu’un utilisateur, un groupe d’utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d’actions des utilisateurs et des rôles peuvent exécuter, sur quelles

ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Exemples de politiques basées sur l'identité pour la gestion des comptes

Pour consulter des exemples de politiques de gestion des comptes basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour AWS la gestion des comptes

Politiques basées sur les ressources dans le cadre de la gestion des comptes

Prend en charge les politiques basées sur les ressources	Non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources

accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Actions politiques pour la gestion des comptes

Prend en charge les actions de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions de gestion de compte, voir Actions définies par la direction des AWS comptes dans la référence d'autorisation de service.

Les actions de politique dans la gestion des comptes utilisent le préfixe suivant avant l'action.

```
account
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "account:action1",
      "account:action2"
         ]
```

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui fonctionnent avec les contacts alternatifs Compte AWS d'un utilisateur, incluez l'action suivante.

```
"Action": "account:*AlternateContact"
```

Pour consulter des exemples de politiques de gestion des comptes basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour AWS la gestion des comptes

Ressources relatives aux politiques pour la gestion des comptes

Prend en charge les ressources de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Le service de gestion des comptes prend en charge les types de ressources spécifiques suivants dans l'`Resource`élément d'une politique IAM afin de vous aider à filtrer la politique et à faire la distinction entre ces types de Comptes AWS :

- account

  Ce `resource` type correspond uniquement aux comptes autonomes Comptes AWS qui ne sont pas membres d'une organisation gérée par le AWS Organizations service.

- accountInOrganization

  Ce `resource` type ne correspond Comptes AWS qu'aux comptes membres d'une organisation gérée par le AWS Organizations service.

Pour consulter la liste des types de ressources de gestion des comptes et de leurs ARN, consultez la section Ressources définies par la gestion des AWS comptes dans la référence d'autorisation de service. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez la section Actions définies par la gestion des AWS comptes.

Pour consulter des exemples de politiques de gestion des comptes basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour AWS la gestion des comptes

Clés de conditions de politique pour la gestion des comptes

Prend en charge les clés de condition de politique spécifiques au service	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Le service de gestion de compte prend en charge les clés de condition suivantes que vous pouvez utiliser pour filtrer avec précision vos politiques IAM :

- compte : TargetRegion

  Cette clé de condition prend un argument qui consiste en une liste de codes de AWS région. Il vous permet de filtrer la politique pour affecter uniquement les actions qui s'appliquent aux régions spécifiées.

- compte : AlternateContactTypes

  Cette clé de condition contient une liste d'autres types de contacts :

  - FACTURATION
  - OPERATIONS
  - SECURITY

  L'utilisation de cette touche vous permet de filtrer la demande uniquement pour les actions qui ciblent les autres types de contact spécifiés.

- compte : AccountResourceOrgPaths

  Cette clé de condition prend un argument qui consiste en une liste d'ARN avec des caractères génériques représentant les comptes d'une organisation. Il vous permet de filtrer la politique pour qu'elle n'affecte que les actions qui ciblent les comptes dont les ARN correspondent. Par exemple, l'ARN suivant correspond uniquement aux comptes de l'organisation spécifiée et de l'unité organisationnelle (UO) spécifiée.

  ```
  arn:aws:account::111111111111:ou/o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/*
  ```

- compte : AccountResourceOrgTags

  Cette clé de condition prend un argument qui consiste en une liste de clés et de valeurs de balise. Il vous permet de filtrer la politique pour qu'elle n'affecte que les comptes membres d'une organisation et qui sont étiquetés avec les clés et les valeurs de balise spécifiées.

Pour consulter la liste des clés de condition de gestion de compte, consultez la section Clés de condition pour la gestion de AWS compte dans la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez la section Actions définies par la gestion du AWS compte.

Pour consulter des exemples de politiques de gestion des comptes basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour AWS la gestion des comptes

Listes de contrôle d'accès dans la gestion des comptes

Prend en charge les listes ACL	Non

Les listes de contrôle d’accès (ACL) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l’autorisation d’accéder à une ressource. Les listes de contrôle d’accès sont similaires aux politiques basées sur les ressources, bien qu’elles n’utilisent pas le format de document de politique JSON.

Contrôle d'accès basé sur les attributs avec gestion de compte

Prend en charge ABAC (étiquettes dans les politiques)	Oui

Le contrôle d’accès par attributs (ABAC) est une stratégie d’autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L’étiquetage des entités et des ressources est la première étape d’ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l’identification du principal correspond à celle de la ressource à laquelle il tente d’accéder.

L’ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l’accès basé sur des étiquettes, vous devez fournir les informations d’étiquette dans l’élément de condition d’une politique utilisant les clés de condition `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur l'ABAC, consultez Qu'est-ce que le contrôle d'accès basé sur les attributs (ABAC) ? dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Utilisation d'informations d'identification temporaires avec la gestion des comptes

Prend en charge les informations d'identification temporaires	Oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Changement de rôle (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Autorisations principales interservices pour la gestion des comptes

Prend en charge les sessions d'accès direct (FAS)	Oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

Rôles de service pour la gestion des comptes

Prend en charge les fonctions de service	Non

Une fonction du service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

Rôles liés aux services pour la gestion des comptes

Prend en charge les rôles liés à un service	Non

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus d'informations sur la création ou la gestion des rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM. Recherchez un service dans le tableau qui inclut un `Yes` dans la colonne Rôle lié à un service. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Exemples de politiques basées sur l'identité pour AWS la gestion des comptes

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources de gestion de compte. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par la gestion des comptes, y compris le format des ARN pour chacun des types de ressources, voir Actions, ressources et clés de condition pour la gestion des AWS comptes dans la référence d'autorisation de service.

Rubriques

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources de gestion de compte dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à

vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.

- Accorder les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

À l'aide de la page Compte du AWS Management Console

Pour accéder à la page Compte dans le AWS Management Console, vous devez disposer d'un minimum d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter les détails de votre Compte AWS. Si vous créez une politique basée sur l'identité qui est plus restrictive

que les autorisations minimales requises, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs et rôles IAM) tributaires de cette politique.

Pour garantir que les utilisateurs et les rôles peuvent utiliser la console de gestion des comptes, vous pouvez choisir d'associer la politique `AWSAccountManagementReadOnlyAccess` ou la politique `AWSAccountManagementFullAccess` AWS gérée aux entités. Pour plus d'informations, consultez Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement la AWS CLI ou l' AWS API. Dans de nombreux cas, vous pouvez plutôt choisir de n'autoriser l'accès qu'aux actions correspondant aux opérations d'API que vous essayez d'effectuer.

Fournir un accès en lecture seule à la page Compte dans le AWS Management Console

Dans l'exemple suivant, vous souhaitez accorder à un utilisateur IAM dans votre compte un accès en Compte AWS lecture seule à la page Compte du. AWS Management Console Les utilisateurs auxquels cette politique est attachée ne peuvent apporter aucune modification.

L'`account:GetAccountInformation`action donne accès à la plupart des paramètres de la page Compte. Toutefois, pour afficher les AWS régions actuellement activées, vous devez également inclure l'`account:ListRegions`action.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GrantReadOnlyAccessToAccountSettings",
            "Effect": "Allow",
            "Action": [
                "account:GetAccountInformation",
                "account:ListRegions"
            ],
            "Resource": "*"
        }
    ]
}
```

Fournir un accès complet à la page Compte dans le AWS Management Console

Dans l'exemple suivant, vous souhaitez accorder à un utilisateur IAM l'accès Compte AWS complet à la page Compte du AWS Management Console. Les utilisateurs auxquels cette politique est attachée peuvent modifier les paramètres du compte.

Cet exemple de stratégie s'appuie sur l'exemple de stratégie précédent en ajoutant chacune des autorisations d'écriture disponibles (à l'exception de CloseAccount), ce qui permet à l'utilisateur de modifier la plupart des paramètres du compte, y compris les `account:DisableRegion` autorisations `account:EnableRegion` et.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GrantFullAccessToAccountSettings",
            "Effect": "Allow",
            "Action": [
                "account:GetAccountInformation",
                "account:ListRegions",
                "account:PutContactInformation",
                "account:PutChallengeQuestions",
                "account:PutAlternateContact",
                "account:DeleteAlternateContact",
                "account:EnableRegion",
                "account:DisableRegion"
            ],
            "Resource": "*"
        }
    ]
}
```

Utilisation de politiques basées sur l'identité (politiques IAM) pour la gestion des comptes AWS

Pour une discussion complète sur les AWS comptes et les utilisateurs IAM, voir Qu'est-ce que l'IAM ? dans le guide de l'utilisateur IAM.

Pour obtenir des instructions sur la mise à jour des stratégies gérées par le client, consultez Editing customer managed policies (console) (Modification des stratégies gérées par le client [console]) dans le guide de l'utilisateur IAM.

AWS Politiques relatives aux actions de gestion des comptes

Ce tableau récapitule les autorisations qui donnent accès aux paramètres de votre compte. Pour des exemples de politiques qui utilisent ces autorisations, consultez la section Exemples de politiques de gestion des AWS comptes.

> **Note**
>
> Pour accorder aux utilisateurs IAM un accès en écriture à un paramètre de compte spécifique sur la page Compte du AWS Management Console, vous devez accorder l'`GetAccountInformation`autorisation, en plus de l'autorisation (ou des autorisations) que vous souhaitez utiliser pour modifier ce paramètre.

Nom de l'autorisation	Niveau d'accès	Description
`account:ListRegions`	Liste	Accorde l'autorisation de répertorier les régions disponibles.
`account:GetAccount Information`	Lecture	Accorde l'autorisation de récupérer les informations de compte d'un compte.
`account:GetAlterna teContact`	Lecture	Accorde l'autorisation de récupérer les contacts alternati fs d'un compte.
`account:GetChallen geQuestions`	Lecture	Accorde l'autorisation de récupérer les questions du défi associées à un compte.
`account:GetContact Information`	Lecture	Accorde l'autorisation de récupérer les informations de contact principales d'un compte.

Nom de l'autorisation	Niveau d'accès	Description
`account:GetRegionOptStatus`	Lecture	Accorde l'autorisation d'obtenir le statut d'opt-in d'une région.
`account:AcceptPrimaryEmailUpdate`	Écrire	Accorde l'autorisation d'accepter la mise à jour de l'adresse e-mail principale du compte membre d'une AWS organisation.
`account:CloseAccount`	Écrire	Accorde l'autorisation de fermer un compte. **Note** Cette autorisation ne s'applique qu'à la console. Aucun accès API n'est disponible pour cette autorisation.
`account:DeleteAlternateContact`	Écrire	Accorde l'autorisation de supprimer les contacts secondaires d'un compte.
`account:DisableRegion`	Écrire	Accorde l'autorisation de désactiver l'utilisation d'une région.
`account:EnableRegion`	Écrire	Accorde l'autorisation d'autoriser l'utilisation d'une région.
`account:PutAlternateContact`	Écrire	Accorde l'autorisation de modifier les contacts alternatifs d'un compte.

Nom de l'autorisation	Niveau d'accès	Description
`account:PutChallengeQuestions`	Écrire	Accorde l'autorisation de modifier les questions du défi pour un compte. **Note** Cette autorisation ne s'applique qu'à la console. Aucun accès API n'est disponible pour cette autorisation.
`account:PutContactInformation`	Écrire	Accorde l'autorisation de mettre à jour les informations de contact principales d'un compte.
`account:StartPrimaryEmailUpdate`	Écrire	Accorde l'autorisation de lancer la mise à jour de l'adresse e-mail principale du compte membre d'une AWS organisation.

Résolution des problèmes d'identité et d'accès à la gestion des AWS comptes

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Account Management et IAM.

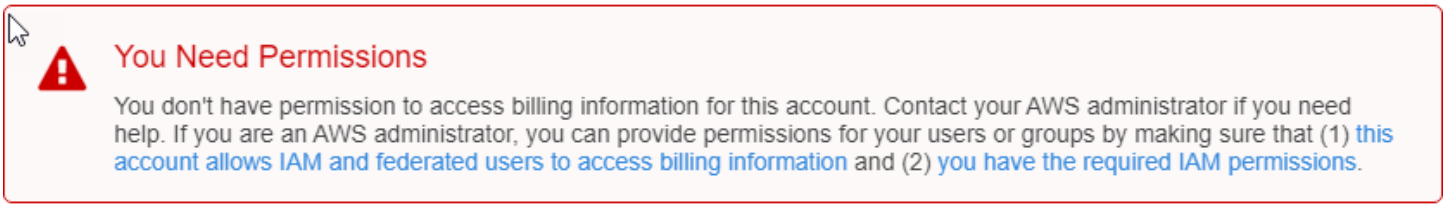
Rubriques

- Je ne suis pas autorisé à effectuer une action sur la page Compte
- Je ne suis pas autorisé à effectuer iam:PassRole
- Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder aux informations de mon compte

Je ne suis pas autorisé à effectuer une action sur la page Compte

S'il vous AWS Management Console indique que vous n'êtes pas autorisé à effectuer une action, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni votre nom d'utilisateur et votre mot de passe.

L'exemple d'erreur suivant se produit lorsque l'utilisateur `mateojackson` IAM essaie d'utiliser la console pour afficher des informations le concernant sur la page Compte du, AWS Management Console mais qu'il ne dispose pas des `account:GetAccountInformation` autorisations nécessaires. Compte AWS



Dans ce cas, Mateo demande à son administrateur de mettre à jour ses politiques pour lui permettre d'accéder à la ressource *`my-example-widget`* à l'aide de l'action `account:`*`GetWidget`*.

Je ne suis pas autorisé à effectuer **`iam:PassRole`**

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transférer un rôle à la gestion du compte.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans la gestion des comptes. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d’identification de connexion.

Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder aux informations de mon compte

Vous pouvez créer un rôle que les utilisateurs provenant d’autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d’accès (ACL), vous pouvez utiliser ces politiques pour donner l’accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si la gestion des comptes prend en charge ces fonctionnalités, consultezComment fonctionne la gestion des AWS comptes avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d’identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d’identité) dans le Guide de l’utilisateur IAM.
- Pour connaître la différence entre l'utilisation de rôles et de politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

AWSpolitiques gérées pourAWSGestion des comptes

AWSLa gestion des comptes fournit actuellement deuxAWSpolitiques gérées qui sont disponibles pour votre utilisation :

- AWS Politique gérée par: AWSAccountManagementReadOnlyAccess
- AWS Politique gérée par: AWSAccountManagementFullAccess
- Mises à jour de la gestion des comptesAWSpolitiques gérées

Une politique gérée par AWS est une politique autonome créée et administrée par AWS. Les politiques gérées par AWS sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

Gardez à l'esprit que les politiques gérées par AWS peuvent ne pas accorder les autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont disponibles pour tous les clients AWS. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les stratégies gérées par AWS. Si AWS met à jour les autorisations définies dans une politique gérée par AWS, la mise à jour affecte toutes les identités de principal (utilisateurs, groupes et rôles) auxquelles la politique est associée. AWS est plus susceptible de mettre à jour une politique gérée par AWS lorsqu'un nouveau Service AWS est lancé ou que de nouvelles opérations API deviennent accessibles pour les services existants.

Pour plus d'informations, consultez la rubrique Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWS Politique gérée par: AWSAccountManagementReadOnlyAccess

Vous pouvez attacher la politique `AWSAccountManagementReadOnlyAccess` à vos identités IAM.

Cette politique fournit des autorisations en lecture seule pour afficher uniquement les éléments suivants :

- Les métadonnées concernant votreComptes AWS
- LeRégions AWSqui sont activés ou désactivés pourCompte AWS(vous pouvez consulter le statut des régions dans votre compte uniquement à l'aide duAWSconsole)

Pour ce faire, il autorise l'exécution de l'un des`Get*`ou`List*`opérations. Il ne permet pas de modifier les métadonnées du compte ni d'activer ou de désactiverRégions AWSpour le compte.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `account`— Permet aux administrateurs de récupérer les informations de métadonnées surComptes AWS. Il permet également aux directeurs d'indiquer lesRégions AWSqui sont activés pour le compte dansAWS Management Console.

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

AWS Politique gérée par: AWSAccountManagementFullAccess

Vous pouvez attacher la politique `AWSAccountManagementFullAccess` à vos identités IAM.

Cette politique fournit un accès administratif complet permettant de consulter ou de modifier les éléments suivants :

- Les métadonnées concernant votreComptes AWS
- LeRégions AWSqui sont activés ou désactivés pourCompte AWS(vous pouvez consulter l'état ou activer ou désactiver les régions pour votre compte uniquement à l'aide duAWSconsole)

Pour ce faire, il autorise l'exécution de n'importe quel`account`opérations.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `account`— Permet aux directeurs d'afficher ou de modifier les informations de métadonnées concernantComptes AWS. Il permet également aux directeurs d'indiquer lesRégions AWSqui sont activées pour le compte et qui sont activées ou désactivées dansAWS Management Console.

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

```
            "Action": "account:*",
            "Resource": "*"
        }
    ]
}
```

Mises à jour de la gestion des comptesAWSpolitiques gérées

Afficher les détails des mises à jour deAWSpolitiques gérées pour la gestion des comptes depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page d'historique des documents de gestion du compte.

Modification	Description	Date
AWSLa gestion des comptes a été lancée avec une nouvelleA WSpolitiques gérées et commencé à suivre les modifications	La gestion des comptes a été initialement lancée avec les éléments suivantsAWSPolitiq ues gérées : • AWSAccountManageme ntReadOnlyAccess • AWSAccountManageme ntFullAccess	30 septembre 2021

Validation de la conformité pour la gestion des AWS comptes

Des auditeurs tiers évaluent la sécurité et la conformité des AWS services que vous pouvez exécuter dans Compte AWS le cadre de plusieurs programmes de AWS conformité. Il s'agit notamment des certifications SOC, PCI, FedRAMP, HIPAA et d'autres.

Pour une liste des AWS services relevant du champ d'application de programmes de conformité spécifiques, voir Services AWSÉtendue par programme de conformité Services AWS . Pour obtenir des renseignements généraux, consultez Programmes de conformité AWS.

Vous pouvez télécharger les rapports de l'audit externe avec AWS Artifact. Pour plus d'informations, consultez la section Téléchargement de rapports dans la section AWS Artifact du Guide de AWS Artifact l'utilisateur. AWS Artifact

Votre responsabilité en matière de conformité lorsque vous utilisez les services que vous utilisez Compte AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWSfournit les ressources suivantes pour faciliter la mise en conformité :

- Guides Quick Start de la sécurité et de la conformité : ces guides de déploiement traitent de considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de référence dans AWS centrés sur la sécurité et la conformité.
- Architecture pour la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent utiliser AWS pour créer des applications éligibles à la loi HIPAA.

> **Note**
>
> Tous les Services AWS ne sont pas éligibles à HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- Ressources de conformité AWS : cet ensemble de manuels et de guides peut s'appliquer à votre secteur d'activité et à votre emplacement.
- Évaluation des ressources à l'aide de règles dans le Guide du développeur AWS Config : le service AWS Config évalue dans quelle mesure vos configurations de ressources sont conformes aux pratiques internes, aux directives sectorielles et aux réglementations.
- AWS Security Hub : ce Service AWS fournit une vue complète de votre état de sécurité au sein d'AWS, ce qui vous permet de vérifier votre conformité aux normes du secteur et aux bonnes pratiques de sécurité.
- AWS Audit Manager – Ce Service AWS vous aide à auditer en continu votre utilisation d'AWS pour simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience dansAWSGestion de compte

LeAWSrepose sur une infrastructure mondiale d'repose surRégions AWSet des zones de disponibilité. Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à débit élevé et à forte redondance. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont

plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les Régions AWS et les zones de disponibilité, consultez Infrastructure mondiale d'AWS.

Sécurité de l'infrastructure dans AWS Account Management

En tant que services gérés, AWS les services exécutés sur votre Compte AWS site sont protégés par la sécurité AWS globale du réseau. Pour plus d'informations sur les services de sécurité AWS et la manière dont AWS protège l'infrastructure, consultez la section Sécurité du cloud AWS. Pour concevoir votre environnement AWS en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le Security Pillar AWS Well-Architected Framework (Pilier de sécurité de l'infrastructure Well-Architected Framework).

Vous utilisez des appels d'API AWS publiés pour accéder aux paramètres du compte via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et nous recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Surveillance de la gestion des AWS comptes

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances de la gestion des AWS comptes et de vos autres AWS solutions. AWSfournit les outils de surveillance suivants pour surveiller la gestion des comptes, signaler tout problème et prendre des mesures automatiques le cas échéant :

- AWS CloudTrailcapture (enregistre) les appels d'API et les événements associés effectués par vous ou en votre nom Compte AWS et écrit les fichiers journaux dans un compartiment Amazon Simple Storage Service (Amazon S3) que vous spécifiez. Cela vous permet d'identifier les utilisateurs et les comptes appelésAWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date à laquelle les appels ont eu lieu. Pour plus d'informations, consultez le AWS CloudTrailGuide de l'utilisateur .
- Amazon EventBridge ajoute une automatisation supplémentaire à vos AWS services en répondant automatiquement aux événements du système, tels que les problèmes de disponibilité des applications ou les modifications des ressources. Les événements AWS liés aux services sont diffusés EventBridge en temps quasi réel. Vous pouvez écrire des règles simples pour préciser les événements qui vous intéressent et les actions automatisées à effectuer quand un événement correspond à une règle. Pour plus d'informations, consultez le guide de EventBridge l'utilisateur Amazon.

JournalisationAWSAppels d'API Gestion de comptes viaAWS CloudTrail

LeAWSLes API de gestion de compte sont intégrées àAWS CloudTrail, un service qui enregistre les actions réalisées par un utilisateur, un rôle ou unAWSservice qui appelle une opération de gestion de compte. CloudTrail capture tous les appels d'API de Gestion de comptes sous forme d'événements. Les appels capturés incluent tous les appels vers les opérations de gestion de compte. Si vous créez un journal d'activité, vous pouvez activer la livraison continue des événements CloudTrail dans un compartiment Amazon S3, y compris des événements pour les opérations de Gestion de comptes. Si vous ne configurez pas de journal d'activité, vous pouvez toujours afficher les événements les plus récents dans la console CloudTrail dans Historique des événements. Avec les informations collectées par CloudTrail, vous pouvez déterminer la demande qui a appelé une opération de gestion de compte, l'adresse IP utilisée pour la demande, l'origine et la date de la demande, ainsi que d'autres détails.

Pour en savoir plus sur CloudTrail, consultez le AWS CloudTrailGuide de l'utilisateur .

Informations sur la gestion de comptes dans CloudTrail

CloudTrail est activé dans votreCompte AWSlorsque vous créez le compte. Lorsqu'une activité a lieu avec une opération de gestion de comptes, celle-ci est enregistrée dans un événement CloudTrail avec d'autres événements CloudTrail avec d'autresAWSévénements de services dansHistorique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre Compte AWS. Pour de plus amples informations, veuillez consulter Affichage des événements avec l'historique des événements CloudTrail.

Pour obtenir un enregistrement continu des événements dans votreCompte AWS, y compris les événements pour les opérations de gestion de comptes, créez un journal d'activité. Un journal d'activité permet à CloudTrail de distribuer les fichiers journaux vers Amazon S3 bucket. Par défaut, lorsque vous créez un journal de suivi dans leAWS Management Console, le sentier s'applique à tousRégions AWS. Le journal d'activité consigne les événements de toutes les Régions dans la partition AWS et livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. Vous pouvez configurer d'autres services AWS afin d'analyser plus en profondeur les données d'événement collectées dans les journaux CloudTrail et d'agir sur celles-ci. Pour en savoir plus, consultez les ressources suivantes :

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

AWS CloudTrailenregistre toutes les opérations de l'API Account Management présentes dans leAPI Referencede ce guide. Par exemple, les appels aux opérations `CreateAccount`, `DeleteAlternateContact` et `PutAlternateContact` génèrent des entrées dans les fichiers journaux CloudTrail.

Chaque événement ou entrée du journal contient des informations sur la personne qui a généré la demande. Les informations relatives à l'identité permettent de déterminer :

- Si la demande a été effectuée avec un utilisateur racine ouAWS Identity and Access Managementinformations d'identification de l'utilisateur (IAM)

- Si la demande a été effectuée avec des informations d'identification de sécurité temporaires pour un rôle IAM ou un utilisateur fédéré
- Si la requête a été effectuée par un autre service AWS

Pour plus d'informations, consultez l'élément userIdentity CloudTrail.

Comprendre les entrées du journal Account Management

Un journal de suivi est une configuration qui permet d'envoyer des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. Les fichiers journaux CloudTrail peuvent contenir une ou plusieurs entrées. Une entrée de journal représente une demande individuelle à partir d'une source quelconque et comprend des informations sur l'opération demandée, y compris la date et l'heure de l'opération, les paramètres de la demande, etc. Les fichiers journaux CloudTrail ne constituent pas une série ordonnée retraçant les appels d'API publiques. Ils ne suivent aucun ordre précis.

Exemple 1 : L'exemple suivant montre une entrée de journal CloudTrail pour un appel vers le`GetAlternateContact`opération pour récupérer le courant`OPERATIONS`contact alternatif pour un compte. Les valeurs renvoyées par l'opération ne sont pas incluses dans les informations consignées.

Example Exemple 1


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA1234567890EXAMPLE:AccountAPITests",
    "arn":"arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA1234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
```

```
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T19:25:53Z"
      }
    }
  },
  "eventTime": "2021-04-30T19:26:15Z",
  "eventSource": "account.amazonaws.com",
  "eventName": "GetAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "alternateContactType": "SECURITY"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-111111111111",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-222222222222",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```


Exemple 2 : L'exemple suivant montre une entrée de journal CloudTrail pour un appel vers le`PutAlternateContact`pour ajouter un nouveau`BILLING`contact alternatif à un compte.


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA1234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA1234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
```

```
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T18:33:00Z"
      }
    }
  },
  "eventTime": "2021-04-30T18:33:08Z",
  "eventSource": "account.amazonaws.com",
  "eventName": "PutAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "name": "*Alejandro Rosalez*",
    "emailAddress": "alrosalez@example.com",
    "title": "CFO",
    "alternateContactType": "BILLING"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-333333333333",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-444444444444",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```

Exemple 3 : L'exemple suivant montre une entrée de journal CloudTrail pour un appel vers le`DeleteAlternateContact`opération pour supprimer le courant`OPERATIONS`contact alternatif.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA1234567890EXAMPLE:AccountAPITests",
    "arn":"arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
```

```
        "type": "Role",
        "principalId": "AROA1234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T18:33:00Z"
      }
    }
  },
  "eventTime": "2021-04-30T18:33:16Z",
  "eventSource": "account.amazonaws.com",
  "eventName": "DeleteAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "alternateContactType": "OPERATIONS"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-555555555555",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-666666666666",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```


Surveillance des événements de gestion des comptes avec EventBridge

Amazon EventBridge, anciennement appelé CloudWatch Events, vous aide à surveiller les événements spécifiques à d'autres et à lancer des actions ciblées qui en utilisent d'autresServices AWS. Les événements de Services AWS sont transmis à EventBridge en temps quasi réel.

À l'aide de EventBridge, vous pouvez créer des règles qui correspondent aux événements entrants et les acheminer vers des cibles à des fins de traitement.

Pour plus d'informations, consultez Getting started with Amazon EventBridge dans le guide de EventBridge l'utilisateur Amazon.

Événements relatifs à la gestion des comptes

Les exemples suivants présentent des événements relatifs à la gestion des comptes. Les événements sont générés sur la base du meilleur effort.

Seuls les événements spécifiques à l'activation et à la désactivation des régions et des appels d'API via CloudTrail sont actuellement disponibles pour la gestion des comptes.

Types d'événements

- Événement d'activation et de désactivation des régions

Événement d'activation et de désactivation des régions

Lorsque vous activez ou désactivez une région dans un compte, que ce soit depuis la console ou depuis l'API, une tâche asynchrone est lancée. La demande initiale sera enregistrée en tant qu' CloudTrail événement dans le compte cible. En outre, un EventBridge événement sera envoyé au compte appelant lorsque le processus d'activation ou de désactivation aura commencé, et à nouveau une fois l'un ou l'autre processus terminé.

L'exemple d'événement suivant montre comment une demande sera envoyée indiquant que `2020-09-30` la `ap-east-1` région était `ENABLED` pour le compte`123456789012`.

```
{
   "version":"0",
   "id":"11112222-3333-4444-5555-666677778888",
   "detail-type":"Region Opt-In Status Change",
   "source":"aws.account",
   "account":"123456789012",
   "time":"2020-09-30T06:51:08Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:account::123456789012:account"
   ],
   "detail":{
      "accountId":"123456789012",
      "regionName":"ap-east-1",
      "status":"ENABLED"
   }
```

```
}
```

Il existe quatre statuts possibles qui correspondent aux statuts renvoyés par les API `GetRegionOptStatus` et `ListRegions` :

- `ENABLED`— La région a été activée avec succès pour le paramètre `accountId` indiqué
- `ENABLING`— La région est en train d'être activée pour les éléments `accountId` indiqués
- `DISABLED`— La région a été désactivée avec succès pour le paramètre `accountId` indiqué
- `DISABLING`— La Région est en train d'être handicapée pour les raisons `accountId` indiquées

L'exemple de modèle d'événements suivant crée une règle qui capture tous les événements régionaux.

```
{
   "source":[
      "aws.account"
   ],
   "detail-type":[
      "Region Opt-In Status Change"
   ]
}
```

L'exemple de modèle d'événements suivant crée une règle qui capture uniquement `ENABLED` les événements `DISABLED` régionaux.

```
{
   "source":[
      "aws.account"
   ],
   "detail-type":[
      "Region Opt-In Status Change"
   ],
   "detail":{
      "status":[
         "DISABLED",
         "ENABLED"
      ]
   }
}
```

Référence API

Les opérations de l'API dans la gestion des comptes (`account`) vous permet de modifier votre espace de nomsCompte AWS.

ChaqueCompte AWSprend en charge les métadonnées contenant des informations sur le compte, y compris des informations sur un maximum de trois contacts alternatifs associés au compte. Elles s'ajoutent à l'adresse e-mail associée auutilisateur rootdu compte. Vous ne pouvez spécifier qu'un seul des types de contact suivants associés à un compte.

- Contact pour la facturation
- Contact pour les opérations
- Contact de sécurité

Par défaut, les opérations d'API décrites dans ce guide s'appliquent directement au compte qui appelle l'opération. Leidentitéle compte qui appelle l'opération se trouve généralement un rôle IAM ou un utilisateur IAM et doit disposer d'une autorisation appliquée par une politique IAM pour appeler l'opération d'API. Vous pouvez également appeler ces opérations d'API à partir d'une identité dans unAWS Organizationscompte de gestion et spécifiez le numéro d'identification du compte pour toutCompte AWSqui est membre de l'organisation.

Version de l'API

Cette version de la référence de l'API Accounts documente la version 2021-02-01 de l'API de gestion des comptes.

> **Note**
>
> Au lieu d'utiliser directement l'API, vous pouvez utiliser l'une desAWSLes kits SDK, qui se composent de bibliothèques et d'exemples de code pour différents langages et plateformes de programmation (Java, Ruby, .NET, iOS, Android, etc.). Les kits SDK constituent un moyen pratique de créer un accès programmatique àAWSOrganisations. Par exemple, les SDK prennent en charge la signature cryptographique des demandes, la gestion des erreurs et la réexécution automatique des demandes. Pour de plus amples informations sur les kits SDK AWS, y compris les procédures pour les télécharger et les installer, consultez Outils pour Amazon Web Services.

Nous vous recommandons d'utiliserAWSSDK pour effectuer des appels d'API programmatiques au service de gestion des comptes. Toutefois, vous pouvez également utiliser l'API Account Management Query pour passer des appels directs au service Web de gestion des comptes. Pour en savoir plus sur l'API Account Management Query, voirAppel de l'API à l'aide de demandes de requête HTTPdans le Guide de l'utilisateur de la gestion des comptes. Les organisations prennent en charge les requêtes GET et POST pour toutes les actions. Autrement dit, l'API ne requiert pas l'utilisation de GET pour certaines actions et de POST pour d'autres. Toutefois, les demandes GET sont soumises aux limitations de taille d'une URL. Par conséquent, pour les opérations nécessitant des tailles plus importantes, utilisez une requête POST.

Signature des requêtes

Lorsque vous envoyez des requêtes HTTP àAWS, vous devez signer les demandes de telle sorte queAWSpeut identifier qui les a envoyés. Vous signez les demandes avec votreAWSclé d'accès, qui se compose d'un identifiant de clé d'accès et d'une clé d'accès secrète. Nous vous recommandons vivement de ne pas créer de clé d'accès pour votre compte root. Toute personne disposant de la clé d'accès à votre compte root a un accès illimité à toutes les ressources de votre compte. Créez plutôt une clé d'accès pour un utilisateur IAM disposant de privilèges administratifs. Comme autre option, utilisezAWSService de jetons de sécurité pour générer des informations d'identification de sécurité temporaires et les utiliser pour signer des demandes.

Pour signer des demandes, nous vous recommandons d'utiliser la version 4 de Signature. Si vous possédez déjà une application qui utilise la version 2 de Signature, il n'est pas nécessaire de la mettre à jour pour utiliser la version 4 de Signature. Toutefois, certaines opérations nécessitent désormais la version 4 de Signature. La documentation relative aux opérations nécessitant la version 4 indique cette exigence. Pour plus d'informations, reportez-vous à Signature des demandes d'API AWS dans le Guide de l'utilisateur IAM.

Lorsque vous utilisezAWSInterface de ligne de commande (AWSCLI) ou l'un desAWSSDK auxquels envoyer des demandesAWS, ces outils signent automatiquement les demandes à votre place à l'aide de la clé d'accès que vous avez spécifiée lors de la configuration des outils.

Assistance et commentaires pour la gestion des comptes

Nous apprécions vos commentaires. Envoyez vos commentaires àfeedback-awsaccounts@amazon.comou publiez vos commentaires et vos questions dansForum d'assistance à la gestion des comptes. Pour de plus amples informations sur les forums de support AWS, consultez Forums Help.

Comment les exemples sont présentés

Le code JSON renvoyé par la gestion du compte en réponse à vos demandes est renvoyé sous la forme d'une longue chaîne unique sans sauts de ligne ni espaces de formatage. Les sauts de ligne et les espaces blancs sont présentés dans les exemples de ce guide afin d'améliorer la lisibilité. Lorsque les paramètres d'entrée d'exemple produiraient également de longues chaînes s'étendant au-delà de l'écran, nous insérons des sauts de ligne pour améliorer la lisibilité. Vous devez toujours soumettre l'entrée sous la forme d'une chaîne de texte JSON unique.

Enregistrement des demandes d'API

Supports de gestion de comptesCloudTrail, un service qui enregistreAWSAppels d'API pour votreCompte AWSet transmet les fichiers journaux à un compartiment Amazon S3. En utilisant les informations collectées parCloudTrail, vous pouvez déterminer quelles demandes ont été envoyées avec succès à la Gestion des comptes, qui a effectué la demande, quand elle a été faite, etc. Pour en savoir plus sur la gestion des comptes et son support pourCloudTrail, voirJournalisationAWSAppels d'API Gestion de comptes viaAWS CloudTrail. Pour en savoir plus surCloudTrail, y compris comment l'activer et trouver vos fichiers journaux, consultez leAWS CloudTrailGuide de l'utilisateur.

Actions

Les actions suivantes sont prises en charge :

- AcceptPrimaryEmailUpdate
- DeleteAlternateContact
- DisableRegion
- EnableRegion
- GetAlternateContact
- GetContactInformation
- GetPrimaryEmail
- GetRegionOptStatus
- ListRegions
- PutAlternateContact
- PutContactInformation
- StartPrimaryEmailUpdate

AcceptPrimaryEmailUpdate

Accepte la demande provenant de la mise StartPrimaryEmailUpdate à jour de l'adresse e-mail principale (également appelée adresse e-mail de l'utilisateur root) pour le compte spécifié.

Syntaxe de la demande

```
POST /acceptPrimaryEmailUpdate HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "Otp": "string",
   "PrimaryEmail": "string"
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

AccountId

Spécifie le numéro d'identification à 12 chiffres du compte Compte AWS auquel vous souhaitez accéder ou modifier lors de cette opération. Pour utiliser ce paramètre, l'appelant doit être une identité enregistrée dans le compte de gestion de l'organisation ou un compte d'administrateur délégué. L'identifiant de compte spécifié doit être un compte membre de la même organisation. Toutes les fonctionnalités de l'organisation doivent être activées et l'organisation doit disposer d'un accès sécurisé activé pour le service de gestion des comptes, et éventuellement d'un compte administrateur délégué attribué.

Cette opération ne peut être appelée que depuis le compte de gestion ou le compte administrateur délégué d'une organisation pour un compte membre.

> **Note**
>
> Le compte de gestion ne peut pas spécifier le sien`AccountId`.

Type : chaîne

Modèle : `^\d{12}$`

Obligatoire : oui

Otp

Le code OTP envoyé à l'adresse `PrimaryEmail` spécifiée lors de l'appel `StartPrimaryEmailUpdate` d'API.

Type : chaîne

Modèle : `^[a-zA-Z0-9]{6}$`

Obligatoire : oui

PrimaryEmail

La nouvelle adresse e-mail principale à utiliser avec le compte spécifié. Cela doit correspondre à celui `PrimaryEmail` de l'appel `StartPrimaryEmailUpdate` d'API.

Type : chaîne

Contraintes de longueur : longueur minimale de 5. Longueur maximale de 64.

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "Status": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

Status

Récupère le statut de la demande de mise à jour par e-mail principale acceptée.

Type : chaîne

Valeurs valides : `PENDING | ACCEPTED`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

AccessDeniedException

L'opération a échoué car l'identité de l'appelant ne dispose pas des autorisations minimales requises.

Code d’état HTTP : 403

ConflictException

La demande n'a pas pu être traitée en raison d'un conflit dans l'état actuel de la ressource. Cela se produit par exemple si vous essayez d'activer une région actuellement désactivée (dont le statut est DÉSACTIVÉ) ou si vous essayez de remplacer l'adresse e-mail de l'utilisateur root d'un compte par une adresse e-mail déjà utilisée.

Code d’état HTTP : 409

InternalServerException

L'opération a échoué en raison d'une erreur interne à AWS. Réessayez l'opération ultérieurement.

Code d’état HTTP : 500

ResourceNotFoundException

L'opération a échoué car elle a spécifié une ressource introuvable.

Code d’état HTTP : 404

TooManyRequestsException

L'opération a échoué car elle a été appelée trop fréquemment et a dépassé la limite d'accélérateur.

Code d’état HTTP : 429

ValidationException

L'opération a échoué car l'un des paramètres d'entrée n'était pas valide.

Code d’état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DeleteAlternateContact

Supprime le contact alternatif spécifié d'un Compte AWS.

Pour plus de détails sur l'utilisation des opérations de contact secondaires, voir Accéder aux contacts secondaires ou les mettre à jour.

> **Note**
>
> Avant de pouvoir mettre à jour les informations de contact secondaires d'une Compte AWS personne gérée par AWS Organizations, vous devez d'abord activer l'intégration entre AWS Account Management et Organizations. Pour plus d'informations, consultez la section Activation de l'accès sécurisé pour la gestion des AWS comptes.

Syntaxe de la demande

```
POST /deleteAlternateContact HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "AlternateContactType": "string"
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

AccountId

Spécifie le numéro d'identification à 12 chiffres du AWS compte auquel vous souhaitez accéder ou modifier à l'aide de cette opération.

Si vous ne spécifiez pas ce paramètre, il s'agit par défaut du AWS compte de l'identité utilisée pour appeler l'opération.

Pour utiliser ce paramètre, l'appelant doit être une identité figurant dans le compte de gestion de l'organisation ou un compte administrateur délégué, et l'identifiant de compte spécifié doit être un compte membre de la même organisation. Toutes les fonctionnalités de l'organisation doivent être activées et l'organisation doit disposer d'un accès sécurisé activé pour le service de gestion des comptes, et éventuellement d'un compte administrateur délégué attribué.

> **Note**
>
> Le compte de gestion ne peut pas spécifier le sien `AccountId` ; il doit appeler l'opération dans un contexte autonome en n'incluant pas le `AccountId` paramètre.

Pour effectuer cette opération sur un compte qui n'est pas membre d'une organisation, ne spécifiez pas ce paramètre et appelez l'opération en utilisant une identité appartenant au compte dont vous souhaitez récupérer ou modifier les contacts.

Type : chaîne

Modèle : `^\d{12}$`

Obligatoire : non

AlternateContactType

Spécifie les contacts alternatifs à supprimer.

Type : chaîne

Valeurs valides : `BILLING | OPERATIONS | SECURITY`

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

AccessDeniedException

L'opération a échoué car l'identité de l'appelant ne dispose pas des autorisations minimales requises.

Code d’état HTTP : 403

InternalServerException

L'opération a échoué en raison d'une erreur interne à AWS. Réessayez l'opération ultérieurement.

Code d’état HTTP : 500

ResourceNotFoundException

L'opération a échoué car elle a spécifié une ressource introuvable.

Code d’état HTTP : 404

TooManyRequestsException

L'opération a échoué car elle a été appelée trop fréquemment et a dépassé la limite d'accélérateur.

Code d’état HTTP : 429

ValidationException

L'opération a échoué car l'un des paramètres d'entrée n'était pas valide.

Code d’état HTTP : 400

Exemples

Exemple 1

L'exemple suivant supprime le contact secondaire de sécurité pour le compte dont les informations d'identification sont utilisées pour appeler l'opération.

Exemple de demande

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.DeleteAlternateContact

{ "AlternateContactType": "SECURITY" }
```

Exemple de réponse

```
HTTP/1.1 200 OK
Content-Type: application/json
```

Exemple 2

L'exemple suivant supprime le contact alternatif de facturation pour le compte membre spécifié dans une organisation. Vous devez utiliser les informations d'identification du compte de gestion de l'organisation ou du compte d'administrateur délégué du service de gestion des comptes.

Exemple de demande

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.DeleteAlternateContact

{ "AccountId": "123456789012", "AlternateContactType": "BILLING" }
```

Exemple de réponse

```
HTTP/1.1 200 OK
Content-Type: application/json
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2

- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DisableRegion

Désactive (désactive) une région spécifique pour un compte.

> **Note**
>
> La désactivation d'une région supprimera tout accès IAM à toutes les ressources résidant dans cette région.

Syntaxe de la demande

```
POST /disableRegion HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "RegionName": "string"
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

AccountId

Spécifie le numéro d'identification à 12 chiffres du compte Compte AWS auquel vous souhaitez accéder ou modifier lors de cette opération. Si vous ne spécifiez pas ce paramètre, il s'agit par défaut du compte Amazon Web Services associé à l'identité utilisée pour appeler l'opération. Pour utiliser ce paramètre, l'appelant doit être une identité enregistrée dans le compte de gestion de l'organisation ou un compte d'administrateur délégué. L'identifiant de compte spécifié doit être un compte membre de la même organisation. Toutes les fonctionnalités de l'organisation doivent être activées et l'organisation doit disposer d'un accès sécurisé activé pour le service de gestion des comptes, et éventuellement d'un compte administrateur délégué attribué.

> **Note**
>
> Le compte de gestion ne peut pas spécifier le sien`AccountId`. Il doit appeler l'opération dans un contexte autonome en n'incluant pas le `AccountId` paramètre.

Pour appeler cette opération sur un compte qui n'est pas membre d'une organisation, ne spécifiez pas ce paramètre. Appelez plutôt l'opération en utilisant une identité appartenant au compte dont vous souhaitez récupérer ou modifier les contacts.

Type : chaîne

Modèle : `^\d{12}$`

Obligatoire : non

RegionName

Spécifie le code de région pour un nom de région donné (par exemple,`af-south-1`). Lorsque vous désactivez une région, AWS exécute des actions pour la désactiver dans votre compte, par exemple en détruisant les ressources IAM de la région. Ce processus prend quelques minutes pour la plupart des comptes, mais cela peut prendre plusieurs heures. Vous ne pouvez pas activer la région tant que le processus de désactivation n'est pas complètement terminé.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 50.

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

AccessDeniedException

L'opération a échoué car l'identité de l'appelant ne dispose pas des autorisations minimales requises.

Code d’état HTTP : 403

ConflictException

La demande n'a pas pu être traitée en raison d'un conflit dans l'état actuel de la ressource. Par exemple, cela se produit si vous essayez d'activer une région actuellement désactivée (dont le statut est DÉSACTIVÉ) ou si vous essayez de remplacer l'adresse e-mail de l'utilisateur root d'un compte par une adresse e-mail déjà utilisée.

Code d’état HTTP : 409

InternalServerException

L'opération a échoué en raison d'une erreur interne à AWS. Réessayez l'opération ultérieurement.

Code d’état HTTP : 500

TooManyRequestsException

L'opération a échoué car elle a été appelée trop fréquemment et a dépassé la limite d'accélérateur.

Code d’état HTTP : 429

ValidationException

L'opération a échoué car l'un des paramètres d'entrée n'était pas valide.

Code d’état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

EnableRegion

Active (opte) une région particulière pour un compte.

Syntaxe de la demande

```
POST /enableRegion HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "RegionName": "string"
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

AccountId

Spécifie le numéro d'identification à 12 chiffres du compte Compte AWS auquel vous souhaitez accéder ou modifier lors de cette opération. Si vous ne spécifiez pas ce paramètre, il s'agit par défaut du compte Amazon Web Services associé à l'identité utilisée pour appeler l'opération. Pour utiliser ce paramètre, l'appelant doit être une identité enregistrée dans le compte de gestion de l'organisation ou un compte d'administrateur délégué. L'identifiant de compte spécifié doit être un compte membre de la même organisation. Toutes les fonctionnalités de l'organisation doivent être activées et l'organisation doit disposer d'un accès sécurisé activé pour le service de gestion des comptes, et éventuellement d'un compte administrateur délégué attribué.

> **Note**
>
> Le compte de gestion ne peut pas spécifier le sien`AccountId`. Il doit appeler l'opération dans un contexte autonome en n'incluant pas le `AccountId` paramètre.

Pour appeler cette opération sur un compte qui n'est pas membre d'une organisation, ne spécifiez pas ce paramètre. Appelez plutôt l'opération en utilisant une identité appartenant au compte dont vous souhaitez récupérer ou modifier les contacts.

Type : chaîne

Modèle : `^\d{12}$`

Obligatoire : non

RegionName

Spécifie le code de région pour un nom de région donné (par exemple,`af-south-1`). Lorsque vous activez une région, AWS effectue des actions pour préparer votre compte dans cette région, telles que la distribution de vos ressources pour la région. Ce processus prend quelques minutes pour la plupart des comptes, mais peut prendre plusieurs heures. Vous ne pouvez pas utiliser la région tant que ce processus n'est pas terminé. En outre, vous ne pouvez pas désactiver la région tant que le processus d'activation n'est pas complètement terminé.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 50.

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

AccessDeniedException

L'opération a échoué car l'identité de l'appelant ne dispose pas des autorisations minimales requises.

Code d’état HTTP : 403

ConflictException

La demande n'a pas pu être traitée en raison d'un conflit dans l'état actuel de la ressource. Cela se produit par exemple si vous essayez d'activer une région actuellement désactivée (dont le statut est DÉSACTIVÉ) ou si vous essayez de remplacer l'adresse e-mail de l'utilisateur root d'un compte par une adresse e-mail déjà utilisée.

Code d’état HTTP : 409

InternalServerException

L'opération a échoué en raison d'une erreur interne à AWS. Réessayez l'opération ultérieurement.

Code d’état HTTP : 500

TooManyRequestsException

L'opération a échoué car elle a été appelée trop fréquemment et a dépassé la limite d'accélérateur.

Code d’état HTTP : 429

ValidationException

L'opération a échoué car l'un des paramètres d'entrée n'était pas valide.

Code d’état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3

- AWS SDK pour Python
- AWS SDK pour Ruby V3

GetAlternateContact

Récupère le contact alternatif spécifié attaché à un Compte AWS.

Pour plus de détails sur l'utilisation des opérations de contact secondaires, voir Accéder aux contacts secondaires ou les mettre à jour.

> **Note**
>
> Avant de pouvoir mettre à jour les informations de contact secondaires d'une Compte AWS personne gérée par AWS Organizations, vous devez d'abord activer l'intégration entre AWS Account Management et Organizations. Pour plus d'informations, consultez la section Activation de l'accès sécurisé pour la gestion des AWS comptes.

Syntaxe de la demande

```
POST /getAlternateContact HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "AlternateContactType": "string"
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

AccountId

Spécifie le numéro d'identification à 12 chiffres du AWS compte auquel vous souhaitez accéder ou modifier avec cette opération.

Si vous ne spécifiez pas ce paramètre, il s'agit par défaut du AWS compte de l'identité utilisée pour appeler l'opération.

Pour utiliser ce paramètre, l'appelant doit être une identité figurant dans le compte de gestion de l'organisation ou un compte administrateur délégué, et l'identifiant de compte spécifié doit être un compte membre de la même organisation. Toutes les fonctionnalités de l'organisation doivent être activées et l'organisation doit disposer d'un accès sécurisé activé pour le service de gestion des comptes, et éventuellement d'un compte administrateur délégué attribué.

> **Note**
>
> Le compte de gestion ne peut pas spécifier le sien `AccountId` ; il doit appeler l'opération dans un contexte autonome en n'incluant pas le `AccountId` paramètre.

Pour effectuer cette opération sur un compte qui n'est pas membre d'une organisation, ne spécifiez pas ce paramètre et appelez l'opération en utilisant une identité appartenant au compte dont vous souhaitez récupérer ou modifier les contacts.

Type : chaîne

Modèle : `^\d{12}$`

Obligatoire : non

AlternateContactType

Spécifie le contact alternatif que vous souhaitez récupérer.

Type : chaîne

Valeurs valides : `BILLING | OPERATIONS | SECURITY`

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "AlternateContact": {
      "AlternateContactType": "string",
      "EmailAddress": "string",
      "Name": "string",
```

```
        "PhoneNumber": "string",
        "Title": "string"
    }
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

AlternateContact

Structure contenant les détails du contact alternatif spécifié.

Type : objet AlternateContact

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

AccessDeniedException

L'opération a échoué car l'identité de l'appelant ne dispose pas des autorisations minimales requises.

Code d'état HTTP : 403

InternalServerException

L'opération a échoué en raison d'une erreur interne à AWS. Réessayez l'opération ultérieurement.

Code d'état HTTP : 500

ResourceNotFoundException

L'opération a échoué car elle a spécifié une ressource introuvable.

Code d'état HTTP : 404

TooManyRequestsException

L'opération a échoué car elle a été appelée trop fréquemment et a dépassé la limite d'accélérateur.

Code d’état HTTP : 429

ValidationException

L'opération a échoué car l'un des paramètres d'entrée n'était pas valide.

Code d’état HTTP : 400

Exemples

Exemple 1

L'exemple suivant récupère le contact de sécurité alternatif pour le compte dont les informations d'identification sont utilisées pour appeler l'opération.

Exemple de demande

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.GetAlternateContact

{ "AlternateContactType": "SECURITY" }
```

Exemple de réponse

```
HTTP/1.1 200 OK
Content-Type: application/json{
   "AlternateContact": {
        "Name": "Anika",
        "Title": "COO",
        "EmailAddress": "anika@example.com",
        "PhoneNumber": "206-555-0198"
        "AlternateContactType": "Security"
    }
}
```

Exemple 2

L'exemple suivant permet de récupérer le contact alternatif des opérations pour le compte membre spécifié dans une organisation. Vous devez utiliser les informations d'identification du compte de gestion de l'organisation ou du compte d'administrateur délégué du service de gestion des comptes.

Exemple de demande

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.GetAlternateContact

{ "AccountId": "123456789012", "AlternateContactType": "Operations" }
```

Exemple de réponse

```
HTTP/1.1 200 OK
Content-Type: application/json{
   "AlternateContact": {
        "Name": "Anika",
        "Title": "COO",
        "EmailAddress": "anika@example.com",
        "PhoneNumber": "206-555-0198"
        "AlternateContactType": "Operations"
    }
}
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

GetContactInformation

Récupère les informations de contact principales d'un Compte AWS.

Pour plus de détails sur l'utilisation des opérations du contact principal, voir Mettre à jour les informations du contact principal et secondaire.

Syntaxe de la demande

```
POST /getContactInformation HTTP/1.1
Content-type: application/json

{
   "AccountId": "string"
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

AccountId

Spécifie le numéro d'identification à 12 chiffres du compte Compte AWS auquel vous souhaitez accéder ou modifier lors de cette opération. Si vous ne spécifiez pas ce paramètre, il s'agit par défaut du compte Amazon Web Services associé à l'identité utilisée pour appeler l'opération. Pour utiliser ce paramètre, l'appelant doit être une identité enregistrée dans le compte de gestion de l'organisation ou un compte d'administrateur délégué. L'identifiant de compte spécifié doit être un compte membre de la même organisation. Toutes les fonctionnalités de l'organisation doivent être activées et l'organisation doit disposer d'un accès sécurisé activé pour le service de gestion des comptes, et éventuellement d'un compte administrateur délégué attribué.

> **Note**
>
> Le compte de gestion ne peut pas spécifier le sien`AccountId`. Il doit appeler l'opération dans un contexte autonome en n'incluant pas le `AccountId` paramètre.

Pour appeler cette opération sur un compte qui n'est pas membre d'une organisation, ne spécifiez pas ce paramètre. Appelez plutôt l'opération en utilisant une identité appartenant au compte dont vous souhaitez récupérer ou modifier les contacts.

Type : chaîne

Modèle : ^\d{12}$

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "ContactInformation": {
      "AddressLine1": "string",
      "AddressLine2": "string",
      "AddressLine3": "string",
      "City": "string",
      "CompanyName": "string",
      "CountryCode": "string",
      "DistrictOrCounty": "string",
      "FullName": "string",
      "PhoneNumber": "string",
      "PostalCode": "string",
      "StateOrRegion": "string",
      "WebsiteUrl": "string"
   }
}
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

ContactInformation

Contient les détails des informations de contact principales associées à un Compte AWS.

Type : objet ContactInformation

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

AccessDeniedException

L'opération a échoué car l'identité de l'appelant ne dispose pas des autorisations minimales requises.

Code d’état HTTP : 403

InternalServerException

L'opération a échoué en raison d'une erreur interne à AWS. Réessayez l'opération ultérieurement.

Code d’état HTTP : 500

ResourceNotFoundException

L'opération a échoué car elle a spécifié une ressource introuvable.

Code d’état HTTP : 404

TooManyRequestsException

L'opération a échoué car elle a été appelée trop fréquemment et a dépassé la limite d'accélérateur.

Code d’état HTTP : 429

ValidationException

L'opération a échoué car l'un des paramètres d'entrée n'était pas valide.

Code d’état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

GetPrimaryEmail

Récupère l'adresse e-mail principale du compte spécifié.

Syntaxe de la demande

```
POST /getPrimaryEmail HTTP/1.1
Content-type: application/json

{
   "AccountId": "string"
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

AccountId

Spécifie le numéro d'identification à 12 chiffres du compte Compte AWS auquel vous souhaitez accéder ou modifier lors de cette opération. Pour utiliser ce paramètre, l'appelant doit être une identité enregistrée dans le compte de gestion de l'organisation ou un compte d'administrateur délégué. L'identifiant de compte spécifié doit être un compte membre de la même organisation. Toutes les fonctionnalités de l'organisation doivent être activées et l'organisation doit disposer d'un accès sécurisé activé pour le service de gestion des comptes, et éventuellement d'un compte administrateur délégué attribué.

Cette opération ne peut être appelée que depuis le compte de gestion ou le compte administrateur délégué d'une organisation pour un compte membre.

> **Note**
>
> Le compte de gestion ne peut pas spécifier le sien`AccountId`.

Type : chaîne

Modèle : ^\d{12}$

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "PrimaryEmail": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

PrimaryEmail

Récupère l'adresse e-mail principale associée au compte spécifié.

Type : chaîne

Contraintes de longueur : longueur minimale de 5. Longueur maximale de 64.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

AccessDeniedException

L'opération a échoué car l'identité de l'appelant ne dispose pas des autorisations minimales requises.

Code d'état HTTP : 403

InternalServerException

L'opération a échoué en raison d'une erreur interne à AWS. Réessayez l'opération ultérieurement.

Code d’état HTTP : 500

ResourceNotFoundException

L'opération a échoué car elle a spécifié une ressource introuvable.

Code d’état HTTP : 404

TooManyRequestsException

L'opération a échoué car elle a été appelée trop fréquemment et a dépassé la limite d'accélérateur.

Code d’état HTTP : 429

ValidationException

L'opération a échoué car l'un des paramètres d'entrée n'était pas valide.

Code d’état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

GetRegionOptStatus

Récupère le statut d'opt-in d'une région donnée.

Syntaxe de la demande

```
POST /getRegionOptStatus HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "RegionName": "string"
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

AccountId

Spécifie le numéro d'identification à 12 chiffres du compte Compte AWS auquel vous souhaitez accéder ou modifier lors de cette opération. Si vous ne spécifiez pas ce paramètre, il s'agit par défaut du compte Amazon Web Services associé à l'identité utilisée pour appeler l'opération. Pour utiliser ce paramètre, l'appelant doit être une identité enregistrée dans le compte de gestion de l'organisation ou un compte d'administrateur délégué. L'identifiant de compte spécifié doit être un compte membre de la même organisation. Toutes les fonctionnalités de l'organisation doivent être activées et l'organisation doit disposer d'un accès sécurisé activé pour le service de gestion des comptes, et éventuellement d'un compte administrateur délégué attribué.

> **Note**
>
> Le compte de gestion ne peut pas spécifier le sien`AccountId`. Il doit appeler l'opération dans un contexte autonome en n'incluant pas le `AccountId` paramètre.

Pour appeler cette opération sur un compte qui n'est pas membre d'une organisation, ne spécifiez pas ce paramètre. Appelez plutôt l'opération en utilisant une identité appartenant au compte dont vous souhaitez récupérer ou modifier les contacts.

Type : chaîne

Modèle : `^\d{12}$`

Obligatoire : non

RegionName

Spécifie le code de région pour un nom de région donné (par exemple,`af-south-1`). Cette fonction renverra le statut de la région que vous passez dans ce paramètre.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 50.

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "RegionName": "string",
   "RegionOptStatus": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

RegionName

Le code de région qui a été transmis.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 50.

RegionOptStatus

L'un des statuts potentiels qu'une région peut subir (Activé, Activant, Désactivé, Désactivant, Enabled_By_Default).

Type : chaîne

Valeurs valides : `ENABLED | ENABLING | DISABLING | DISABLED | ENABLED_BY_DEFAULT`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

AccessDeniedException

L'opération a échoué car l'identité de l'appelant ne dispose pas des autorisations minimales requises.

Code d’état HTTP : 403

InternalServerException

L'opération a échoué en raison d'une erreur interne à AWS. Réessayez l'opération ultérieurement.

Code d’état HTTP : 500

TooManyRequestsException

L'opération a échoué car elle a été appelée trop fréquemment et a dépassé la limite d'accélérateur.

Code d’état HTTP : 429

ValidationException

L'opération a échoué car l'un des paramètres d'entrée n'était pas valide.

Code d’état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListRegions

Répertorie toutes les régions associées à un compte donné et leurs statuts d'inscription respectifs. Cette liste peut éventuellement être filtrée par le `region-opt-status-contains` paramètre.

Syntaxe de la demande

```
POST /listRegions HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "MaxResults": number,
   "NextToken": "string",
   "RegionOptStatusContains": [ "string" ]
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

AccountId

Spécifie le numéro d'identification à 12 chiffres du compte Compte AWS auquel vous souhaitez accéder ou modifier lors de cette opération. Si vous ne spécifiez pas ce paramètre, il s'agit par défaut du compte Amazon Web Services associé à l'identité utilisée pour appeler l'opération. Pour utiliser ce paramètre, l'appelant doit être une identité enregistrée dans le compte de gestion de l'organisation ou un compte d'administrateur délégué. L'identifiant de compte spécifié doit être un compte membre de la même organisation. Toutes les fonctionnalités de l'organisation doivent être activées et l'organisation doit disposer d'un accès sécurisé activé pour le service de gestion des comptes, et éventuellement d'un compte administrateur délégué attribué.

> **Note**
>
> Le compte de gestion ne peut pas spécifier le sien`AccountId`. Il doit appeler l'opération dans un contexte autonome en n'incluant pas le `AccountId` paramètre.

Pour appeler cette opération sur un compte qui n'est pas membre d'une organisation, ne spécifiez pas ce paramètre. Appelez plutôt l'opération en utilisant une identité appartenant au compte dont vous souhaitez récupérer ou modifier les contacts.

Type : chaîne

Modèle : `^\d{12}$`

Obligatoire : non

MaxResults

Le nombre total d'éléments à renvoyer dans la sortie de la commande. Si le nombre total d'éléments disponibles est supérieur à la valeur spécifiée, un `NextToken` est fourni dans la sortie de la commande. Pour reprendre la pagination, fournissez la valeur de `NextToken` dans l'argument `starting-token` d'une commande suivante. N'utilisez pas l'élément de `NextToken` réponse directement en dehors de la AWS CLI. Pour des exemples d'utilisation, voir Pagination dans le guide de l'utilisateur de l'interface de ligne de AWS commande.

Type : entier

Plage valide : valeur minimum de 1. Valeur maximale de 50.

Obligatoire : non

NextToken

Un jeton utilisé pour indiquer où commencer la pagination. Il s'agit du `NextToken` résultat d'une réponse tronquée précédemment. Pour des exemples d'utilisation, voir Pagination dans le guide de l'utilisateur de l'interface de ligne de AWS commande.

Type : chaîne

Contraintes de longueur : longueur minimale de 0. Longueur maximum de 1 000.

Obligatoire : non

RegionOptStatusContains

Liste des statuts des régions (Activation, Activé, Désactivé, Désactivé, Activé par défaut) à utiliser pour filtrer la liste des régions pour un compte donné. Par exemple, la transmission d'une valeur ENABLING renverra uniquement une liste de régions dont le statut de région est ENABLING.

Type : tableau de chaînes

Valeurs valides : `ENABLED | ENABLING | DISABLING | DISABLED | ENABLED_BY_DEFAULT`

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Regions": [
      {
         "RegionName": "string",
         "RegionOptStatus": "string"
      }
   ]
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

NextToken

Si d'autres données doivent être renvoyées, elles seront renseignées. Il doit être transmis dans le paramètre de `next-token` requête de`list-regions`.

Type : chaîne

Regions

Il s'agit d'une liste de régions pour un compte donné ou, si le paramètre filtré a été utilisé, d'une liste de régions correspondant aux critères de filtre définis dans le `filter` paramètre.

Type : tableau d'objets Region

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

AccessDeniedException

L'opération a échoué car l'identité de l'appelant ne dispose pas des autorisations minimales requises.

Code d’état HTTP : 403

InternalServerException

L'opération a échoué en raison d'une erreur interne à AWS. Réessayez l'opération ultérieurement.

Code d’état HTTP : 500

TooManyRequestsException

L'opération a échoué car elle a été appelée trop fréquemment et a dépassé la limite d'accélérateur.

Code d’état HTTP : 429

ValidationException

L'opération a échoué car l'un des paramètres d'entrée n'était pas valide.

Code d’état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript

- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

PutAlternateContact

Modifie le contact alternatif spécifié attaché à un Compte AWS.

Pour plus de détails sur l'utilisation des opérations de contact secondaires, voir Accéder aux contacts secondaires ou les mettre à jour.

> **Note**
>
> Avant de pouvoir mettre à jour les informations de contact secondaires d'une Compte AWS personne gérée par AWS Organizations, vous devez d'abord activer l'intégration entre AWS Account Management et Organizations. Pour plus d'informations, consultez la section Activation de l'accès sécurisé pour la gestion des AWS comptes.

Syntaxe de la demande

```
POST /putAlternateContact HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "AlternateContactType": "string",
   "EmailAddress": "string",
   "Name": "string",
   "PhoneNumber": "string",
   "Title": "string"
}
```

Paramètres de demande URI

La demande n’utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

AccountId

Spécifie le numéro d'identification à 12 chiffres du AWS compte auquel vous souhaitez accéder ou modifier à l'aide de cette opération.

Si vous ne spécifiez pas ce paramètre, il s'agit par défaut du AWS compte de l'identité utilisée pour appeler l'opération.

Pour utiliser ce paramètre, l'appelant doit être une identité figurant dans le compte de gestion de l'organisation ou un compte administrateur délégué, et l'identifiant de compte spécifié doit être un compte membre de la même organisation. Toutes les fonctionnalités de l'organisation doivent être activées et l'organisation doit disposer d'un accès sécurisé activé pour le service de gestion des comptes, et éventuellement d'un compte administrateur délégué attribué.

> **Note**
>
> Le compte de gestion ne peut pas spécifier le sien `AccountId` ; il doit appeler l'opération dans un contexte autonome en n'incluant pas le `AccountId` paramètre.

Pour effectuer cette opération sur un compte qui n'est pas membre d'une organisation, ne spécifiez pas ce paramètre et appelez l'opération en utilisant une identité appartenant au compte dont vous souhaitez récupérer ou modifier les contacts.

Type : chaîne

Modèle : `^\d{12}$`

Obligatoire : non

AlternateContactType

Spécifie le contact alternatif que vous souhaitez créer ou mettre à jour.

Type : chaîne

Valeurs valides : `BILLING | OPERATIONS | SECURITY`

Obligatoire : oui

EmailAddress

Spécifie l'adresse e-mail de l'autre contact.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 254.

Modèle : `^[\s]*[\w+=.#|!&-]+@[\w.-]+\.[\w]+[\s]*$`

Obligatoire : oui

Name

Spécifie le nom de l'autre contact.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 64.

Obligatoire : oui

PhoneNumber

Spécifie le numéro de téléphone de l'autre contact.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 25

Modèle : `^[\s0-9()+-]+$`

Obligatoire : oui

Title

Spécifie le titre de l'autre contact.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 50.

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

AccessDeniedException

L'opération a échoué car l'identité de l'appelant ne dispose pas des autorisations minimales requises.

Code d’état HTTP : 403

InternalServerException

L'opération a échoué en raison d'une erreur interne à AWS. Réessayez l'opération ultérieurement.

Code d’état HTTP : 500

TooManyRequestsException

L'opération a échoué car elle a été appelée trop fréquemment et a dépassé la limite d'accélérateur.

Code d’état HTTP : 429

ValidationException

L'opération a échoué car l'un des paramètres d'entrée n'était pas valide.

Code d’état HTTP : 400

Exemples

Exemple 1

L'exemple suivant définit le contact alternatif de facturation pour le compte dont les informations d'identification sont utilisées pour appeler l'opération.

Exemple de demande

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.PutAlternateContact

{
```

```
    "AlternateContactType": "Billing",
    "Name": "Carlos Salazar",
    "Title": "CFO",
    "EmailAddress": "carlos@example.com",
    "PhoneNumber": "206-555-0199"
}
```

Exemple de réponse

```
HTTP/1.1 200 OK
Content-Type: application/json
```

Exemple 2

L'exemple suivant définit ou remplace le contact de facturation alternatif pour le compte de membre spécifié dans une organisation. Vous devez utiliser les informations d'identification du compte de gestion de l'organisation ou du compte d'administrateur délégué du service de gestion des comptes.

Exemple de demande

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.PutAlternateContact

{
    "AccountId": "123456789012",
    "AlternateContactType": "Billing",
    "Name": "Carlos Salazar",
    "Title": "CFO",
    "EmailAddress": "carlos@example.com",
    "PhoneNumber": "206-555-0199"
}
```

Exemple de réponse

```
HTTP/1.1 200 OK
Content-Type: application/json
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

PutContactInformation

Met à jour les informations de contact principales d'un Compte AWS.

Pour plus de détails sur l'utilisation des opérations du contact principal, voir Mettre à jour les informations du contact principal et secondaire.

Syntaxe de la demande

```
POST /putContactInformation HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "ContactInformation": {
      "AddressLine1": "string",
      "AddressLine2": "string",
      "AddressLine3": "string",
      "City": "string",
      "CompanyName": "string",
      "CountryCode": "string",
      "DistrictOrCounty": "string",
      "FullName": "string",
      "PhoneNumber": "string",
      "PostalCode": "string",
      "StateOrRegion": "string",
      "WebsiteUrl": "string"
   }
}
```

Paramètres de demande URI

La demande n’utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

AccountId

Spécifie le numéro d'identification à 12 chiffres du compte Compte AWS auquel vous souhaitez accéder ou modifier lors de cette opération. Si vous ne spécifiez pas ce paramètre, il s'agit par

défaut du compte Amazon Web Services associé à l'identité utilisée pour appeler l'opération. Pour utiliser ce paramètre, l'appelant doit être une identité enregistrée dans le compte de gestion de l'organisation ou un compte d'administrateur délégué. L'identifiant de compte spécifié doit être un compte membre de la même organisation. Toutes les fonctionnalités de l'organisation doivent être activées et l'organisation doit disposer d'un accès sécurisé activé pour le service de gestion des comptes, et éventuellement d'un compte administrateur délégué attribué.

> **Note**
>
> Le compte de gestion ne peut pas spécifier le sien`AccountId`. Il doit appeler l'opération dans un contexte autonome en n'incluant pas le `AccountId` paramètre.

Pour appeler cette opération sur un compte qui n'est pas membre d'une organisation, ne spécifiez pas ce paramètre. Appelez plutôt l'opération en utilisant une identité appartenant au compte dont vous souhaitez récupérer ou modifier les contacts.

Type : chaîne

Modèle : `^\d{12}$`

Obligatoire : non

ContactInformation

Contient les détails des informations de contact principales associées à un Compte AWS.

Type : objet ContactInformation

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

AccessDeniedException

L'opération a échoué car l'identité de l'appelant ne dispose pas des autorisations minimales requises.

Code d’état HTTP : 403

InternalServerException

L'opération a échoué en raison d'une erreur interne à AWS. Réessayez l'opération ultérieurement.

Code d’état HTTP : 500

TooManyRequestsException

L'opération a échoué car elle a été appelée trop fréquemment et a dépassé la limite d'accélérateur.

Code d’état HTTP : 429

ValidationException

L'opération a échoué car l'un des paramètres d'entrée n'était pas valide.

Code d’état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript

- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

StartPrimaryEmailUpdate

Lance le processus de mise à jour de l'adresse e-mail principale du compte spécifié.

Syntaxe de la demande

```
POST /startPrimaryEmailUpdate HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "PrimaryEmail": "string"
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

AccountId

Spécifie le numéro d'identification à 12 chiffres du compte Compte AWS auquel vous souhaitez accéder ou modifier lors de cette opération. Pour utiliser ce paramètre, l'appelant doit être une identité enregistrée dans le compte de gestion de l'organisation ou un compte d'administrateur délégué. L'identifiant de compte spécifié doit être un compte membre de la même organisation. Toutes les fonctionnalités de l'organisation doivent être activées et l'organisation doit disposer d'un accès sécurisé activé pour le service de gestion des comptes, et éventuellement d'un compte administrateur délégué attribué.

Cette opération ne peut être appelée que depuis le compte de gestion ou le compte d'administrateur délégué d'une organisation pour un compte membre.

> **Note**
>
> Le compte de gestion ne peut pas spécifier le sien`AccountId`.

Type : chaîne

Modèle : `^\d{12}$`

Obligatoire : oui

PrimaryEmail

La nouvelle adresse e-mail principale (également appelée adresse e-mail de l'utilisateur root) à utiliser dans le compte spécifié.

Type : chaîne

Contraintes de longueur : longueur minimale de 5. Longueur maximale de 64.

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "Status": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

Status

État de la demande de mise à jour par e-mail principale.

Type : chaîne

Valeurs valides : `PENDING | ACCEPTED`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

AccessDeniedException

L'opération a échoué car l'identité de l'appelant ne dispose pas des autorisations minimales requises.

Code d’état HTTP : 403

ConflictException

La demande n'a pas pu être traitée en raison d'un conflit dans l'état actuel de la ressource. Cela se produit par exemple si vous essayez d'activer une région actuellement désactivée (dont le statut est DÉSACTIVÉ) ou si vous essayez de remplacer l'adresse e-mail de l'utilisateur root d'un compte par une adresse e-mail déjà utilisée.

Code d’état HTTP : 409

InternalServerException

L'opération a échoué en raison d'une erreur interne à AWS. Réessayez l'opération ultérieurement.

Code d’état HTTP : 500

ResourceNotFoundException

L'opération a échoué car elle a spécifié une ressource introuvable.

Code d’état HTTP : 404

TooManyRequestsException

L'opération a échoué car elle a été appelée trop fréquemment et a dépassé la limite d'accélérateur.

Code d’état HTTP : 429

ValidationException

L'opération a échoué car l'un des paramètres d'entrée n'était pas valide.

Code d’état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

Actions associées dans d'autresAWSservices

Les opérations suivantes sont liées àAWS Account Managementmais font partie duAWS Organizationsespace de noms :

- CreateAccount
- Créer un compte Gov Cloud
- DescribeAccount

CreateAccount

Le`CreateAccount`L'opération API peut être utilisée uniquement dans le contexte d'une organisation gérée par leAWS Organizationsservice. L'opération API est définie dans l'espace de noms de ce service.

Pour de plus amples informations, veuillez consulterCreateAccountdans leAWS OrganizationsAPI Reference.

Créer un compte Gov Cloud

Le`CreateGovCloudAccount`L'opération API peut être utilisée uniquement dans le contexte d'une organisation gérée par leAWS Organizationsservice. L'opération API est définie dans l'espace de noms de ce service.

Pour de plus amples informations, veuillez consulterCréer un compte Gov Clouddans leAWS OrganizationsAPI Reference.

DescribeAccount

Le`DescribeAccount`L'opération API peut être utilisée uniquement dans le contexte d'une organisation gérée par leAWS Organizationsservice. L'opération API est définie dans l'espace de noms de ce service.

Pour de plus amples informations, veuillez consulterDescribeAccountdans leAWS OrganizationsAPI Reference.

Types de données

Les types de données suivants sont pris en charge :

- AlternateContact
- ContactInformation
- Region
- ValidationExceptionField

AlternateContact

Structure contenant les détails d'un contact alternatif associé à un AWS compte

Table des matières

AlternateContactType

Type de contact alternatif.

Type : chaîne

Valeurs valides : `BILLING | OPERATIONS | SECURITY`

Obligatoire : non

EmailAddress

Adresse e-mail associée à cet autre contact.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 254

Modèle : `^[\s]*[\w+=.#|!&-]+@[\w.-]+\.[\w]+[\s]*$`

Obligatoire : non

Name

Le nom associé à cet autre contact.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 64.

Obligatoire : non

PhoneNumber

Le numéro de téléphone associé à cet autre contact.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 25

Modèle : `^[\s0-9()+-]+$`

Obligatoire : non

Title

Le titre associé à ce contact alternatif.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 50.

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

ContactInformation

Contient les détails des informations de contact principales associées à un Compte AWS.

Table des matières

AddressLine1

La première ligne de l'adresse du contact principal.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 60.

Obligatoire : oui

City

Ville de l'adresse de contact principale.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 50.

Obligatoire : oui

CountryCode

Le code de pays à deux lettres ISO-3166 pour l'adresse de contact principale.

Type : chaîne

Contraintes de longueur : longueur fixe de 2.

Obligatoire : oui

FullName

Nom complet de l'adresse de contact principale.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 50.

Obligatoire : oui

PhoneNumber

Le numéro de téléphone des coordonnées principales. Le numéro sera validé et, dans certains pays, vérifié pour l'activation.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 20.

Modèle : `^[+][\s0-9()-]+$`

Obligatoire : oui

PostalCode

Le code postal de l'adresse de contact principale.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 20.

Obligatoire : oui

AddressLine2

Deuxième ligne de l'adresse du contact principal, le cas échéant.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 60.

Obligatoire : non

AddressLine3

Troisième ligne de l'adresse du contact principal, le cas échéant.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 60.

Obligatoire : non

CompanyName

Le nom de l'entreprise associée aux coordonnées principales, le cas échéant.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 50.

Obligatoire : non

DistrictOrCounty

Le district ou le comté de l'adresse de contact principale, le cas échéant.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 50.

Obligatoire : non

StateOrRegion

État ou région de l'adresse du contact principal. Si l'adresse postale se trouve aux États-Unis, la valeur de ce champ peut être un code d'État à deux caractères (par exemple,`NJ`) ou le nom complet de l'État (par exemple,`New Jersey`). Ce champ est obligatoire dans les pays suivants : `US`,`CA`,`GB`,`DE`,`JP`,`IN`, et`BR`.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 50.

Obligatoire : non

WebsiteUrl

URL du site Web associée aux coordonnées principales, le cas échéant.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 256.

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

Region

Il s'agit d'une structure qui exprime la région pour un compte donné, composée d'un nom et d'un statut d'opt-in.

Table des matières

RegionName

Le code de région d'une région donnée (par exemple,`us-east-1`).

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 50.

Obligatoire : non

RegionOptStatus

L'un des statuts potentiels qu'une région peut subir (Activé, Activant, Désactivé, Désactivant, Enabled_By_Default).

Type : chaîne

Valeurs valides : `ENABLED | ENABLING | DISABLING | DISABLED | ENABLED_BY_DEFAULT`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

ValidationExceptionField

L'entrée n'a pas satisfait aux contraintes spécifiées par le AWS service dans un champ spécifié.

Table des matières

message

Un message concernant l'exception de validation.

Type : chaîne

Obligatoire : oui

name

Nom du champ dans lequel l'entrée non valide a été détectée.

Type : chaîne

Obligatoire : oui

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

Paramètres communs

La liste suivante contient les paramètres que toutes les actions utilisent pour signer les demandes Signature Version 4 à l'aide d'une chaîne de requête. Tous les paramètres spécifiques d'une action particulière sont énumérées dans le sujet consacré à cette action. Pour plus d'informations sur Signature version 4, consultez la section Signature de demandes d'AWSAPI dans le Guide de l'utilisateur IAM.

Action

Action à effectuer.

Type : chaîne

Obligatoire : oui

Version

Version de l'API pour laquelle la demande est écrite, au format AAAA-MM-JJ.

Type : chaîne

Obligatoire : oui

X-Amz-Algorithm

Algorithme de hachage que vous avez utilisé pour créer la signature de la demande.

Condition : spécifiez ce paramètre lorsque vous incluez des informations d'authentification dans une chaîne de requête plutôt que dans l'en-tête d'autorisation HTTP.

Type : chaîne

Valeurs valides : `AWS4-HMAC-SHA256`

Obligatoire : Conditionnelle

X-Amz-Credential

Valeur de la portée des informations d'identification, qui est une chaîne incluant votre clé d'accès, la date, la région cible, le service demandé et une chaîne de terminaison (« aws4_request »). Spécifiez la valeur au format suivant : access_key/AAAAMMJJ/région/service/aws4_request.

Pour plus d'informations, consultez la section Création d'une demande d'AWSAPI signée dans le Guide de l'utilisateur IAM.

Condition : spécifiez ce paramètre lorsque vous incluez des informations d'authentification dans une chaîne de requête plutôt que dans l'en-tête d'autorisation HTTP.

Type : chaîne

Obligatoire : Conditionnelle

X-Amz-Date

La date utilisée pour créer la signature. Le format doit être au format de base ISO 8601 (AAAAMMJJ'T'HHMMSS'Z'). Par exemple, la date/heure suivante est une valeur X-Amz-Date valide : `20120325T120000Z`.

Condition : X-Amz-Date est un en-tête facultatif pour toutes les demandes. Il peut être utilisé pour remplacer la date dans la signature des demandes. Si l'en-tête Date est spécifié au format de base ISO 8601, X-Amz-Date n'est pas obligatoire. Lorsque X-Amz-Date est utilisé, il remplace toujours la valeur de l'en-tête Date. Pour plus d'informations, consultez la section Éléments d'une signature de demande d'AWSAPI dans le Guide de l'utilisateur IAM.

Type : chaîne

Obligatoire : Conditionnelle

X-Amz-Security-Token

Le jeton de sécurité temporaire obtenu lors d'un appel àAWS Security Token Service (AWS STS). Pour obtenir la liste des services prenant en charge les informations d'identification de sécurité temporaires deAWS STS, consultez la section Services AWSqui fonctionnent avec IAM dans le Guide de l'utilisateur IAM.

Condition : si vous utilisez des informations d'identification de sécurité temporaires deAWS STS, vous devez inclure le jeton de sécurité.

Type : chaîne

Obligatoire : Conditionnelle

X-Amz-Signature

Spécifie la signature codée en hexadécimal qui a été calculée à partir de la chaîne à signer et de la clé de signature dérivée.

Condition : spécifiez ce paramètre lorsque vous incluez des informations d'authentification dans une chaîne de requête plutôt que dans l'en-tête d'autorisation HTTP.

Type : chaîne

Obligatoire : Conditionnelle

X-Amz-SignedHeaders

Spécifie tous les en-têtes HTTP qui ont été inclus dans la demande canonique. Pour plus d'informations sur la spécification d'en-têtes signés, consultez la section Création d'une demande d'AWSAPI signée dans le Guide de l'utilisateur IAM.

Condition : spécifiez ce paramètre lorsque vous incluez des informations d'authentification dans une chaîne de requête plutôt que dans l'en-tête d'autorisation HTTP.

Type : chaîne

Obligatoire : Conditionnelle

Erreurs courantes

Cette section répertorie les erreurs communes aux actions d'API de tous les services AWS. Pour les erreurs spécifiques à une action d'API pour ce service, consultez la rubrique pour cette action d'API.

AccessDeniedException

Vous ne disposez pas d'un accès suffisant pour effectuer cette action.

Code d'état HTTP : 400

IncompleteSignature

La signature de la requête n'est pas conforme aux normes AWS.

Code d'état HTTP : 400

InternalFailure

Le traitement de la demande a échoué en raison d'une erreur, d'une exception ou d'un échec inconnu.

Code d'état HTTP : 500

InvalidAction

L'action ou l'opération demandée n'est pas valide. Vérifiez que l'action est entrée correctement.

Code d'état HTTP : 400

InvalidClientTokenId

Le certificat X.509 ou l'ID de clé d'accès AWS fourni(e) n'existe pas dans nos archives.

Code d'état HTTP : 403

NotAuthorized

Vous ne disposez pas de l'autorisation nécessaire pour effectuer cette action.

Code d'état HTTP : 400

OptInRequired

L'ID de clé d'accès AWS a besoin d'un abonnement pour le service.

Code d'état HTTP : 403

RequestExpired

La demande a atteint le service plus de 15 minutes après la date affichée sur la demande ou plus de 15 minutes après la date d'expiration de la demande (comme pour les URL pré-signées) ou la date affichée sur la demande est postérieure de 15 minutes.

Code d'état HTTP : 400

ServiceUnavailable

La requête a échoué en raison d'une défaillance temporaire du serveur.

HTTP Status Code: 503

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

Code d'état HTTP : 400

ValidationError

L'entrée ne satisfait pas les contraintes spécifiées par un service AWS.

Code d'état HTTP : 400

Appel de l'API à l'aide de demandes de requête HTTP

Cette section contient des informations générales sur l'utilisation de l'API Query pourAWSGestion des comptes. Pour plus d'informations sur le fonctionnement de l'API et les erreurs, consultez le Référence API.

> **Note**
>
> Au lieu de passer des appels directs auAWSAPI Account Management Query, vous pouvez utiliser l'une desAWSSDK. Les kits SDK AWS se composent de bibliothèques et d'exemples de code pour différents langages de programmation et plateformes (Java, Ruby, .NET, iOS, Android, etc). Les kits SDK constituent un moyen pratique de créer un accès programmatique àAWSGestion des comptes etAWS. Par exemple, ils automatisent les tâches telles que la signature cryptographique des demandes, la gestion des erreurs et les nouvelles tentatives automatiques de demande. Pour en savoir plus sur les kits de développement logiciel AWS, y compris les procédures pour les télécharger et les installer, consultez Outils pour Amazon Web Services.

Avec l'API Query pourAWSGestion du compte, vous pouvez appeler des actions de service. Les requêtes de l'API Query sont des requêtes HTTPS qui doivent contenir un`Action`paramètre pour indiquer l'opération à effectuer.AWS Supports de gestion de comptes`GET`et`POST`demandes pour toutes les opérations. C'est-à-dire que l'API ne vous oblige pas à utiliser`GET`pour certaines actions et`POST`pour les autres. Toutefois,`GET`les demandes sont soumises à la limite de taille d'une URL. Bien que cette limite dépende du navigateur, une limite standard est de 2 048 octets. Par conséquent, pour les requêtes de l'API Query qui nécessitent des tailles plus importantes, vous devez utiliser`POST`demande.

Vous obtenez une réponse sous la forme d'un document XML. Pour plus d'informations sur la réponse, consultez les pages d'actions individuelles dans le Référence API.

Rubriques

- Points de terminaison
- HTTPS requis
- SignatureAWSDemandes d'API de gestion de compte

Points de terminaison

AWSLa gestion des comptes possède un point de terminaison d'API mondial unique qui est hébergé dans l'est des États-Unis (Virginie du Nord)Région AWS.

Pour de plus amples informations sur les points de terminaison et les régions AWS pour tous les services, veuillez consulter Régions et points de terminaison dans le Références générales AWS.

HTTPS requis

Étant donné que l'API Query peut renvoyer des informations sensibles telles que des informations d'identification de sécurité, vous devez utiliser le protocole HTTPS pour crypter toutes les demandes d'API.

SignatureAWSDemandes d'API de gestion de compte

Les demandes doivent être signées à l'aide d'un identifiant de la clé d'accès et d'une clé d'accès secrète. Nous vous recommandons vivement de ne pas utiliser votreAWSinformations d'identification du compte root pour le travail quotidien avecAWSGestion des comptes. Vous pouvez utiliser les informations d'identification pourAWS Identity and Access Managementidentifiant utilisateur (IAM) ou informations d'identification temporaires telles que celles que vous utilisez avec un rôle IAM.

Pour signer vos demandes d'API, vous devez utiliser AWS Signature Version 4. Pour plus d'informations sur l'utilisation de Signature Version 4, consultez la rubrique Signature des demandes d'API AWS du Guide de l'utilisateur IAM.

Pour plus d'informations, consultez les ressources suivantes :

- Informations d'identification de sécurité AWS : fournit des informations générales sur les types d'informations d'identification que vous pouvez utiliser pour accéder à AWS.
- Bonnes pratiques de sécurité dans IAM— Propose des suggestions pour utiliser le service IAM afin de sécuriser votreAWSressources, y compris celles figurant dansAWSGestion des comptes.
- Informations d'identification de sécurité temporaires dans IAM : décrit comment créer et utiliser des informations d'identification de sécurité temporaires.

Quotas pour AWS Account Management

Votre Compte AWS dispose de quotas par défaut, anciennement appelés limites, pour chaque service AWS. Sauf indication contraire, chaque quota est Région AWS spécifique.

Chacun Compte AWS dispose des quotas suivants liés à la gestion des comptes.

Ressource	Quota
Nombre de contacts alternatifs dans un Compte AWS	3 - un pour chaque `BILLINGSECURITY`, et `OPERATIONS`
Nombre de demandes d'option de région simultanées par compte	6
Nombre de demandes d'option de région simultanées par organisation	20
Taux de `DeleteAlternateContact` demandes par compte	1 par seconde, rafale à 6 par seconde
Taux de `DisableRegion` demandes par compte	1 par seconde, rafale à 1 par seconde
Taux de `EnableRegion` demandes par compte	1 par seconde, rafale à 1 par seconde
Taux de `GetAlternateContact` demandes par compte	10 par seconde, rafale à 15 par seconde
Taux de `GetContactInformation` demandes par compte	10 par seconde, rafale à 15 par seconde
Taux de `GetRegionOptStatus` demandes par compte	5 par seconde, rafale à 5 par seconde
Taux de `ListRegions` demandes par compte	5 par seconde, rafale à 5 par seconde

Ressource	Quota
Taux de `PutAlternateContact` demandes par compte	5 par seconde, rafale à 8 par seconde
Taux de `PutContactInformation` demandes par compte	5 par seconde, rafale à 8 par seconde

Dépannage de votre Compte AWS

Utilisez les informations contenues dans les rubriques suivantes pour vous aider à diagnostiquer et à résoudre les problèmes liés à votreCompte AWS. Pour obtenir de l'aide concernant l'utilisateur root, consultez la section Résolution des problèmes liés à l'utilisateur root dans le Guide de l'utilisateur IAM. Pour obtenir de l'aide concernant le processus de connexion, consultez la section Résolution des problèmes de Compte AWS connexion dans le Guide de l'utilisateur de AWSconnexion.

Résolution des problèmes liés aux rubriques

- Résolution des problèmes liés à Compte AWS la création
- Résolution des problèmes liés à Compte AWS la fermeture
- Résolution des problèmes liés àComptes AWS

Résolution des problèmes liés à Compte AWS la création

Utilisez les liens de référence du tableau suivant pour vous aider à diagnostiquer et à résoudre les problèmes liés à la création d'un nouveau Compte AWS.

Problème	Lien de référence	Source
Je ne sais pas comment m'inscrire ou créer un compte	Création d'un appareil autonome Compte AWS	Ce guide
Que dois-je faire si je n'ai pas reçu d'appel AWS pour vérifier que mon nouveau compte ou si le code PIN que j'ai saisi ne fonctionne pas ?	https://repost.aws/knowledge-center/ phone-verify-no-call	AWS re:Post
Comment puis-je résoudre l'erreur « nombre maximum de tentatives infructueuses » lorsque j'essaie de vérifier mon identité Compte AWS par téléphone ?	https://repost.aws/knowledge-center/ maximum-failed-attempts	AWS re:Post

Problème	Lien de référence	Source
Cela fait plus de 24 heures et mon compte n'est pas activé	https://repost.aws/knowledge-center/ create-and-activate-aws -account	AWS re:Post
Je n'arrive pas à me connecter à mon nouveau compte une fois qu'il a été créé	https://docs.aws.amazon.com/signin/latest/userguide/troubleshooting-sign-in-issues .html	AWS Guide de l'utilisateur pour se connecter

Pour obtenir de l'aide supplémentaire, nous vous recommandons de AWS re:Postrechercher du contenu lié à votre problème spécifique. Si vous avez toujours besoin d'assistance, contactez AWS Support.

Résolution des problèmes liés à Compte AWS la fermeture

Utilisez les informations ci-dessous pour vous aider à diagnostiquer et à résoudre les problèmes courants rencontrés lors du processus de fermeture du compte. Pour obtenir des informations générales sur le processus de fermeture du compte, consultezFermez un Compte AWS.

Rubriques

- Je ne sais pas comment supprimer ou annuler mon compte
- Je ne vois pas le bouton Fermer le compte sur la page Comptes
- J'ai fermé mon compte mais je n'ai toujours pas reçu d'e-mail de confirmation
- Je reçois un message d'erreur ConstraintViolationException « » lorsque j'essaie de fermer mon compte
- Je reçois un message d'erreur « CLOSE_ACCOUNT_QUOTA_EXCEDED » lorsque j'essaie de fermer un compte membre
- Dois-je supprimer mon AWS organisation avant de fermer le compte de gestion ?

Je ne sais pas comment supprimer ou annuler mon compte

Pour fermer votre compte, suivez les instructions indiquées dansFermez un Compte AWS.

Je ne vois pas le bouton Fermer le compte sur la page Comptes

Si vous n'êtes pas connecté en tant qu'utilisateur root, le bouton Fermer le compte ne s'affichera pas sur la page Comptes. Vous devez vous connecter en AWS Management Console tant qu'utilisateur root pour fermer votre compte. Si vous ne parvenez pas à vous connecter, consultez la section Résolution des problèmes liés à l'utilisateur root.

J'ai fermé mon compte mais je n'ai toujours pas reçu d'e-mail de confirmation

Cet e-mail de confirmation est uniquement envoyé à l'adresse e-mail de l'utilisateur root pour le Compte AWS. Si vous ne recevez pas cet e-mail dans les heures qui suivent, vous pouvez vous connecter en AWS Management Console tant qu'utilisateur root pour vérifier que votre compte est fermé. Si votre compte a été fermé avec succès, vous verrez un message indiquant que votre compte est fermé. Si le compte que vous avez fermé est un compte membre, vous pouvez vérifier que la fermeture a bien été effectuée en vérifiant si le compte fermé est étiqueté comme `SUSPENDED` dans la AWS Organizations console. Pour plus d'informations, consultez la rubrique Clôture d'un compte membre de votre organisation du Guide de l'utilisateurAWS Organizations .

Si vous essayez de fermer un compte de gestion et que vous ne recevez pas d'e-mail de confirmation concernant la fermeture du compte, il est fort probable que votre organisation possède des comptes de membres actifs. Vous ne pouvez fermer le compte de gestion que si votre organisation ne possède aucun compte membre actif. Pour vérifier qu'il ne reste aucun compte membre actif dans votre organisation, accédez à la AWS Organizations console et assurez-vous que tous les comptes membres apparaissent à `Suspended` côté de leur nom de compte. Ensuite, vous pouvez fermer le compte de gestion.

Je reçois un message d'erreur ConstraintViolationException « » lorsque j'essaie de fermer mon compte

Vous essayez de fermer un compte de gestion à l'aide de la AWS Organizations console, ce qui n'est pas possible. Pour fermer un compte de gestion, vous devez vous connecter en AWS Management Console tant qu'utilisateur root du compte de gestion et le fermer depuis la page Comptes. Pour plus d'informations, consultez la section Fermeture d'un compte de gestion dans votre organisation dans le Guide deAWS Organizations l'utilisateur.

Je reçois un message d'erreur « CLOSE_ACCOUNT_QUOTA_EXCEDED » lorsque j'essaie de fermer un compte membre

Vous ne pouvez clôturer que 10 % des comptes membres au cours d'une période continue de 30 jours. Ce quota n'est pas lié au mois civil, mais commence lorsque vous fermez un compte. Dans les 30 jours suivant la fermeture initiale du compte, vous ne pouvez pas dépasser la limite de 10 %. La clôture minimale de compte est de 10 et la fermeture maximale de 1 000 comptes, même si 10 % des comptes dépassent 1 000. Pour plus d'informations sur les quotas des Organisations, consultez la section Quotas du Guide deAWS Organizations l'utilisateur. AWS Organizations

Dois-je supprimer mon AWS organisation avant de fermer le compte de gestion ?

Non, il n'est pas nécessaire de supprimer votre AWS organisation avant de fermer le compte de gestion. Toutefois, vous ne pouvez fermer le compte de gestion que si votre organisation ne possède aucun compte membre actif. Pour vérifier qu'il ne reste aucun compte membre actif dans votre organisation, accédez à la AWS Organizations console et assurez-vous que tous les comptes membres apparaissent à `Suspended` côté de leur nom de compte. Ensuite, vous pouvez fermer le compte de gestion.

Résolution des problèmes liés àComptes AWS

Utilisez les informations ici pour vous aider à résoudre les problèmes liés àCompte AWS.

Problèmes

- Je dois changer la carte bancaire de monCompte AWS
- Je dois signaler une fraudeCompte AWSactivité
- Je dois fermer monCompte AWS

Je dois changer la carte bancaire de monCompte AWS

Pour changer la carte bancaire de votreCompte AWS, vous devez pouvoir vous connecter.AWSdispose de protections qui vous obligent à prouver que vous êtes le propriétaire du compte. Pour obtenir des instructions, consultezGestion de vos moyens de paiement par carte de paiementdans leAWS BillingGuide de l'utilisateur.

Je dois signaler une fraudeCompte AWSactivité

Si vous soupçonnez une activité frauduleuse utilisant votreCompte AWSet j'aimerais faire un rapport, voirComment signaler un abus deAWSressources.

Si vous rencontrez des problèmes avec un achat effectué sur Amazon.com, voirService client d'Amazon.

Je dois fermer monCompte AWS

Pour obtenir de l'aide pour résoudre les problèmes liés à la fermeture de votreCompte AWS, voirFermez un Compte AWS.

Historique des documents pour le guide de l'utilisateur de gestion de compte

Le tableau suivant décrit les versions de documentation relatives à la gestion des AWS comptes.

Modification	Description	Date
Nouvelles API de messagerie principales	Support des nouvelles `GetPrimaryEmail` `AcceptPrimaryEmailUpdate` API et `StartPrimaryEmailUpdate` des API pour mettre à jour de manière centralisée l'adresse e-mail de l'utilisateur root pour tout compte membre dans AWS Organizations. Pour plus d'informations, consultez la section Mise à jour de l'adresse e-mail de l'utilisateur root pour un compte de membre dans le Guide de AWS Organizations l'utilisateur.	6 juin 2024
Réécriture de la rubrique relative à la clôture du compte	L'ensemble de la rubrique relative à la clôture des comptes a été entièrement revu, y compris l'ajout d'étapes expliquant comment fermer les comptes des membres et des comptes de gestion.	1 février 2024
Fin du support pour l'ajout de nouvelles questions relatives aux défis de sécurité	Ajout d'un nouveau contenu indiquant que l'option permettant d'ajouter de	5 janvier 2024

	nouvelles questions de défi a été supprimée de la page des comptes.	
Fin du support pour l'espace de `aws-portal` noms	AWS Identity and Access Management Les actions (IAM) précédemment utilisées pour gérer votre compte (par exemple, `aws-portal:ModifyAccount` et `aws-portal:ViewAccount`) ont atteint la fin du support standard.	1er janvier 2024
Réécriture du thème « Régions »	L'ensemble de la rubrique Régions a été complètement remanié, y compris l'ajout de commandes d'extension et de réduction.	8 octobre 2023
Rubriques relatives aux utilisateurs root déplacées vers le guide de l'utilisateur IAM	Discussion consolidée sur les utilisateurs root en une seule rubrique, ajout de liens de références croisées vers des sujets relatifs aux utilisateurs root qui ont été déplacés vers le guide de l'utilisateur IAM.	18 septembre 2023
Nouvelle section ajoutée à la rubrique de contact du compte principal	Ajout d'une nouvelle section sur les exigences relatives au numéro de téléphone et à l'adresse e-mail.	12 septembre 2023
Nouvelles API d'informations de contact	Support pour les nouveautés `GetContactInformation` et `PutContactInformation` les API.	22 juillet 2022

AWS La gestion des comptes prend désormais en charge la mise à jour des contacts alternatifs via la AWS Organizations console.	Vous pouvez désormais mettre à jour les contacts alternatifs de votre organisation via la AWS Organizations console à l'aide des autorisations de l'API de compte fournies par les politiques AWS Organizations gérées mises à jour.	8 février 2022
Première version	Publication initiale du guide de référence AWS sur la gestion des comptes	30 septembre 2021

Glossaire AWS

Pour connaître la terminologie la plus récente d'AWS, consultez le Glossaire AWS dans la Référence Glossaire AWS.

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