Guide de référence

AWS Gestion du compte

AWS Gestion du compte: Guide de référence

Table of Contents

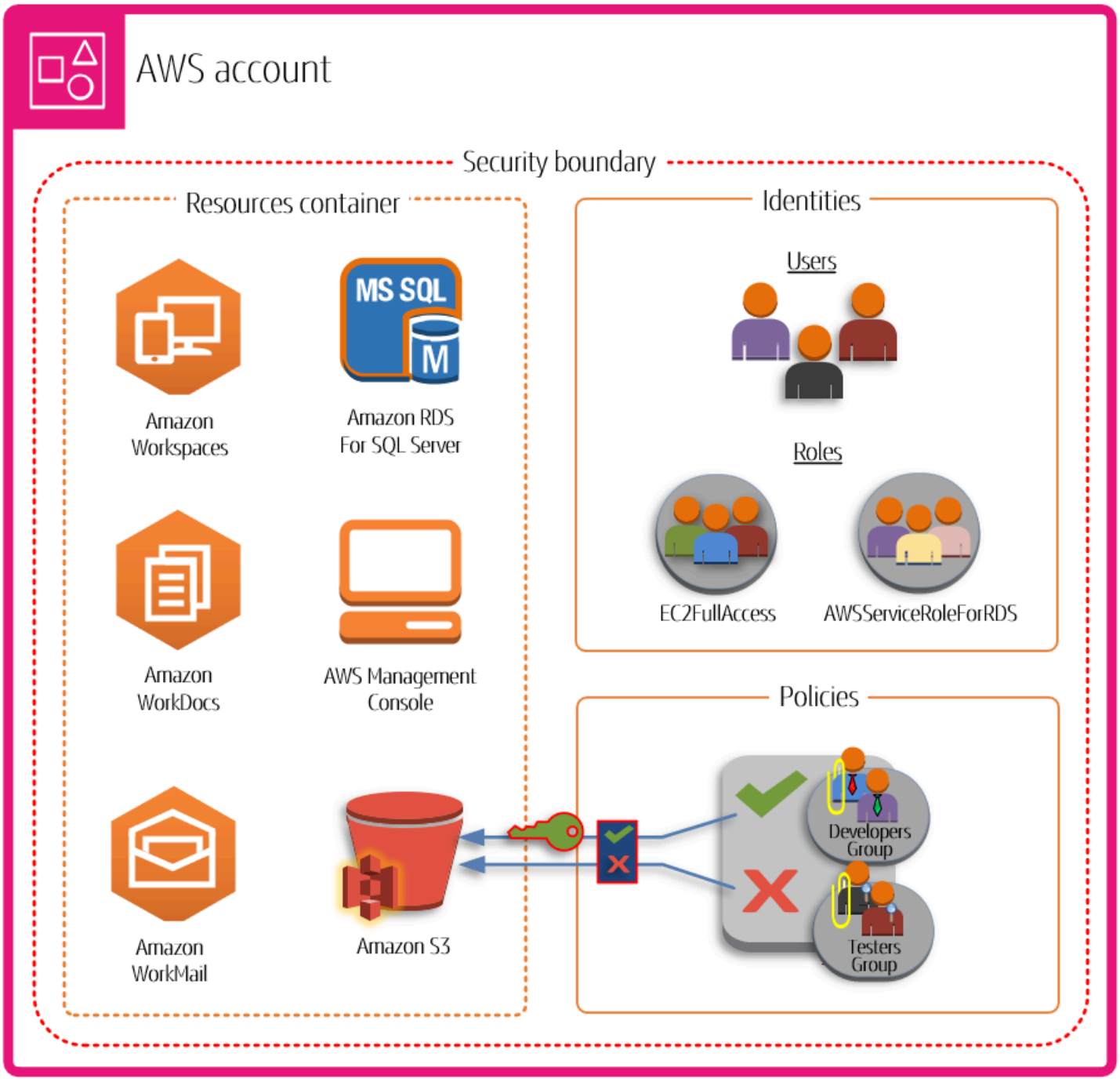
Qu'est-ce qu'un Compte AWS ?

An Compte AWS représente une relation commerciale officielle avec laquelle vous établissez AWS. Vous créez et gérez vos AWS ressources dans un Compte AWS, et votre compte fournit des fonctionnalités de gestion des identités pour l'accès et la facturation. Chacun Compte AWS possède un identifiant unique qui le différencie des autres Comptes AWS.

Vos ressources et données cloud sont contenues dans un Compte AWS. Un compte agit comme une limite d'isolation pour la gestion des identités et des accès. Lorsque vous devez partager des ressources et des données entre deux comptes, vous devez explicitement autoriser cet accès. Par défaut, aucun accès n'est autorisé entre les comptes. Par exemple, si vous désignez différents comptes pour contenir vos ressources et données de production et non liées à la production, aucun accès n'est autorisé entre ces environnements par défaut.

Comptes AWS sont également un élément fondamental de l'accès aux AWS services. Comme le montre l'illustration suivante, un homme Compte AWS remplit deux fonctions principales :

- Conteneur de ressources — 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 (EC2Amazon) sont toutes des ressources. Chaque ressource est identifiée de manière unique par un Amazon Resource Name (ARN) qui inclut l'identifiant 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'authentifier AWS). Les identités ont également des politiques d'autorisation qui spécifient ce qu'un utilisateur peut faire (autorisation) avec les ressources du compte.



L'utilisation de plusieurs Comptes AWS est une bonne pratique pour faire évoluer votre environnement, car elle fournit une limite de facturation naturelle pour les coûts, isole les ressources pour des raisons de sécurité, donne de la flexibilité aux individus et aux équipes, en plus de s'adapter aux nouveaux processus métier. Pour de plus amples informations, veuillez consulter Avantages de l'utilisation de plusieurs Comptes AWS.

Caractéristiques d'un Compte AWS

Comptes AWS incluent les fonctionnalités de base suivantes :

- Surveiller et contrôler les coûts — Un compte est le moyen par défaut d'allocation des AWS coûts. De ce fait, l'utilisation de différents comptes pour différentes unités commerciales et différents groupes de charges de travail peut vous aider à suivre, contrôler, prévoir, budgétiser et signaler plus facilement vos dépenses liées au cloud. Outre le reporting des coûts au niveau du compte, il dispose AWS également d'un support intégré pour consolider et signaler les coûts sur l'ensemble de votre ensemble de comptes si vous choisissez de les utiliser à un AWS Organizations moment ou à un autre. Vous pouvez également utiliser les Quotas de AWS Service pour vous protéger contre le provisionnement excessif et inattendu de AWS ressources et les actions malveillantes susceptibles d'avoir un impact considérable sur vos AWS coûts.
- Unité d'isolation — Une Compte AWS fournit des limites de sécurité, d'accès et de facturation pour vos AWS ressources, ce qui peut vous aider à atteindre l'autonomie et l'isolation des ressources. De par leur conception, toutes les ressources mises en service dans un compte sont logiquement isolées des ressources mises en service dans d'autres comptes, même au sein de votre propre environnement. AWS Cette limite d'isolation vous permet de limiter les risques liés à un problème lié à une application, à une mauvaise configuration ou à des actions malveillantes. Si un problème survient au sein d'un compte, les répercussions sur les charges de travail contenues dans d'autres comptes peuvent être réduites ou éliminées.
- Représentez les charges de travail de votre entreprise : utilisez plusieurs comptes pour regrouper les charges de travail ayant un objectif commercial commun dans des comptes distincts. Ainsi, vous pouvez aligner la propriété et la prise de décision sur ces comptes et éviter les dépendances et les conflits liés à la manière dont les charges de travail des autres comptes sont sécurisées et gérées. En fonction de votre modèle commercial global, vous pouvez choisir d'isoler des unités commerciales ou des filiales distinctes dans différents comptes. Cette approche pourrait également faciliter la cession de ces unités au fil du temps.

Utilisez-vous pour la première fois AWS ?

Si vous utilisez pour la première fois AWS, la première étape consiste à vous inscrire à un Compte AWS. Lorsque vous vous inscrivez, AWS créez un compte avec les informations que vous fournissez et vous attribuez le compte. Après avoir créé votre Compte 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.

Pour step-by-step obtenir des instructions sur la création d'un nouveau compte, consultezCommencer avec un Compte AWS.

AWS Services connexes

Comptes AWS fonctionnent parfaitement avec les services suivants :

- IAM

  Compte AWS Le vôtre est étroitement intégré à AWS Identity and Access Management (IAM). Vous pouvez utiliser IAM avec votre compte pour garantir que les autres personnes travaillant sur votre compte disposent de l'accès dont elles ont besoin pour accomplir leur travail. Vous utilisez également IAM pour contrôler l'accès à toutes vos AWS ressources, et pas uniquement aux informations spécifiques au compte. Il est important que vous vous familiarisiez avec les principaux concepts et les meilleures pratiques de l'IAM avant d'aller trop loin dans la configuration de votre Compte AWS structure. Pour plus d’informations, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l’utilisateur IAM.

- AWS Organizations

  Si votre entreprise est grande ou susceptible de croître, vous souhaiterez peut-être configurer plusieurs AWS comptes qui reflètent la structure spécifique de votre entreprise. AWS Organizations fournit l'infrastructure et les fonctionnalités sous-jacentes qui vous permettent de créer et de gérer vos environnements multi-comptes. Vous pouvez combiner vos comptes existants en une organisation qui vous permet de gérer les comptes de manière centralisée. Vous pouvez créer des comptes qui font automatiquement partie de votre organisation et inviter d'autres comptes à rejoindre votre organisation. Vous pouvez également attacher des politiques qui concernent tous vos comptes ou certains d'entre eux. Pour de plus amples informations, veuillez consulter Quand utiliser AWS Organizations.

- AWS Control Tower

  AWS Control Tower fournit un moyen simplifié de configurer et de gérer un AWS environnement multi-comptes sécurisé. AWS Control Tower automatise la création de votre environnement multi-comptes en instanciant un ensemble de comptes initiaux et en utilisant AWS Organizations des garde-fous et des configurations par défaut pour l'environnement. Vous pouvez l'utiliser AWS Control Tower pour en provisionner de nouveaux Comptes AWS en quelques étapes tout en vous assurant que les comptes sont conformes aux politiques de votre organisation. Pour de plus amples informations, veuillez consulter Quand utiliser AWS Control Tower.

À l'aide du Utilisateur racine d'un compte AWS

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

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

> **Important**
>
> Toute personne disposant de vos identifiants d'utilisateur root Compte AWS a un accès illimité à toutes les ressources de votre compte, y compris aux informations de facturation.

Vous pouvez modifier ou réinitialiser le mot de passe de l'utilisateur root, et créer ou supprimer des clés d'accès (clé d'accès IDs 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.

Support pour la gestion des AWS comptes

Vous pouvez publier des commentaires et des questions via le forum d'assistance à la gestion des AWS comptes. Pour des informations générales sur AWS les forums, consultez AWS re:Post.

Si vous ne trouvez pas les réponses que vous recherchez AWS re:Post, vous pouvez créer un compte ou un dossier d'assistance lié à la facturation à l'aide du AWS Management Console. Pour plus d'informations, voir Exemple : création d'un dossier d'assistance pour le compte et la facturation.

Autres AWS ressources

- AWS Formations et cours — Liens vers des cours spécialisés et basés sur les rôles, ainsi que vers des ateliers d'autoformation pour vous aider à perfectionner vos AWS compétences et à acquérir une expérience pratique.
- AWS Outils de développement : liens vers des outils et des ressources de développement qui fournissent de la documentation, des exemples de code, des notes de publication et d'autres informations pour vous aider à créer des applications innovantes avec AWS.
- AWS Support Centre — Le centre de création et de gestion de vos dossiers de AWS Support. Comprend également des liens vers d'autres ressources utiles, telles que des forums, des informations techniques FAQs, l'état de santé des services et AWS Trusted Advisor.
- AWS Support : page Web principale contenant des informations sur le AWS support one-on-one, un canal d'assistance rapide destiné à vous aider à créer et à exécuter des applications dans le cloud.
- Contactez-nous — Un point de contact central pour les demandes concernant la AWS facturation, le compte, les événements, les abus et autres problèmes.
- AWS Conditions du site — Informations détaillées sur nos droits d'auteur et notre marque commerciale ; votre compte, votre licence et l'accès au site ; et d'autres sujets.

Commencer avec un Compte AWS

Si vous êtes nouveau AWS, la première étape consiste à vous inscrire à un Compte AWS. Lorsque vous le ferez, vous AWS créerez un compte en utilisant les informations que vous fournissez et vous l'attribuerez.

Les rubriques de cette section vous aideront à commencer à découvrir et à configurer un nouveau Compte AWS.

Rubriques

Conditions préalables à la création d'un nouveau Compte AWS

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

- Adresse e-mail de l'utilisateur root Adresse — L'adresse e-mail est utilisée comme nom de connexion pour l'utilisateur root et est requise pour récupérer le 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.

- AWS nom du 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 les identifier facilement. 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).

- Adresse — Si votre adresse de contact et de facturation se trouvent en Inde, le contrat d'utilisation de votre compte est conclu avec Amazon Web Services India Private Limited (AWS Inde), un vendeur AWS local en Inde. Vous devez fournir votre valeur CVV dans le cadre du processus de vérification. Vous devrez peut-être également saisir un mot de passe à usage unique, selon votre banque. AWS L'Inde facture 2 INR à votre mode de paiement dans le cadre du processus de vérification. AWS L'Inde rembourse les 2 INR une fois la vérification terminée.
- 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.

Créez un Compte AWS

Cette rubrique explique comment créer un appareil autonome Compte AWS qui n'est pas géré par AWS Organizations. Si vous souhaitez créer un compte faisant partie d'une organisation gérée par AWS 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, Créez un accord Compte AWS avec AWS l'Inde voir.

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 compte Compte 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 au Compte AWS, vous ne pourrez pas récupérer l'accès au compte en cas de perte du 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. AWS nécessite 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 ! @ # $ % ^ & * () <> [] {} | _ + - =
   - Il ne doit pas être identique à votre Compte AWS nom ou à votre adresse e-mail.

6. Choisissez Professionnel ou Personnel. Les comptes personnels et les comptes professionnels présentent les mêmes caractéristiques et fonctions.
7. Entrez les informations personnelles ou relatives à votre entreprise.

> **Important**
>
> Pour les entreprises Comptes AWS, il est recommandé de participer aux activités suivantes :

- 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 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 Support plans.
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 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 de 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.

Activez 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 en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   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, voir Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur administrateur

Comme il n'est pas possible de 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.

Accès à votre Compte AWS

Vous pouvez accéder Compte AWS à votre de l'une des manières suivantes :

AWS Management Console

AWS Management Console Il s'agit d'une interface basée sur un navigateur que vous pouvez utiliser pour gérer vos Compte AWS paramètres et vos AWS ressources.

AWS Outils de ligne de commande

Avec les outils de ligne de AWS commande, vous pouvez émettre des commandes sur la ligne de commande de votre système pour exécuter Compte AWS des AWS tâches. L'utilisation de la ligne de commande peut être plus rapide et plus pratique que la console. Les outils de ligne de commande sont également utiles si vous souhaitez créer des scripts qui exécutent AWS des tâches. AWS fournit deux ensembles d'outils de ligne de commande :

- AWS Command Line Interface(AWS CLI). Pour plus d'informations sur l'installation et l'utilisation du AWS CLI, consultez le guide de AWS Command Line Interface l'utilisateur.
- AWS Tools for Windows PowerShell. Pour plus d'informations sur l'installation et l'utilisation des outils pour Windows PowerShell, consultez le guide de AWS Tools for Windows PowerShell l'utilisateur.

AWS SDKs

Il AWS SDKs s'agit de bibliothèques et d'exemples de code pour différents langages de programmation et plateformes (par exemple, Java, Python, Ruby, .NET, iOS et Android). Ils se SDKs chargent de tâches telles que la signature cryptographique des demandes, la gestion des erreurs et le renouvellement automatique des demandes. Pour plus d'informations sur les AWS

SDKs, notamment sur la manière de les télécharger et de les installer, consultez la section Outils pour Amazon Web Services.

AWS API de requête HTTPS pour la gestion des comptes

L'API de requête HTTPS de gestion de AWS compte vous donne un accès programmatique à votre Compte AWS et AWS. L'API de requête HTTPS vous permet d'envoyer des demandes HTTPS directement au service. Lorsque vous utilisez l'API HTTPS, vous devez inclure du code pour signer numériquement les demandes à l'aide de vos informations d'identification. Pour plus d'informations, consultez la section Appel de l'API en effectuant des requêtes HTTP.

Planifiez votre structure Compte AWS de gouvernance

Bien que vous ayez commencé votre AWS parcours avec un seul compte, il est AWS recommandé de configurer plusieurs comptes à mesure que vos charges de travail augmentent en taille et en complexité. Que vous soyez une moyenne ou une grande entreprise, vous devez créer un plan de structure de gouvernance qui garantira que vos besoins en matière de données et de charge de travail sont satisfaits.

Cette section couvre les avantages et les services de gouvernance disponibles AWS pour aider à mettre en place une structure de gouvernance multi-comptes.

Rubriques

Avantages de l'utilisation de plusieurs Comptes AWS

Comptes AWS constituent la limite de sécurité fondamentale dans le AWS Cloud. Ils servent de conteneur pour les ressources, fournissant une couche d'isolation essentielle à la création d'un environnement sécurisé et bien gouverné. Pour de plus amples informations, veuillez consulter Qu'est-ce qu'un Compte AWS ?.

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

- Contrôle de sécurité — Les différentes applications peuvent avoir des profils de sécurité différents, ce qui nécessite des politiques et des mécanismes de contrôle différents. Par exemple, il est beaucoup plus facile de parler à un auditeur et de trouver un auditeur Compte AWS qui héberge tous les éléments de votre charge de travail soumis aux normes de sécurité de l'industrie des cartes de paiement (PCI).
- Isolation — An Compte AWS est une unité de protection de sécurité. Les risques potentiels et les menaces de sécurité doivent être maîtrisés à l'intérieur et Compte AWS sans affecter les autres. Les besoins de sécurité peuvent être différents en raison des différentes équipes ou des différents profils de sécurité.

- De nombreuses équipes — Les différentes équipes ont des responsabilités et des besoins en ressources différents. Vous pouvez empêcher les équipes d'interférer les unes avec les autres en les Comptes AWS séparant.
- Isolation des données — En plus d'isoler les équipes, il est important d'isoler les magasins de données d'un compte. Cela peut contribuer à limiter le nombre de personnes pouvant accéder à ce magasin de données et le gérer. Cela permet de limiter l'exposition à des données hautement privées et peut donc contribuer au respect du règlement général sur la protection des données (RGPD) de l'Union européenne.
- Processus métier — Des unités commerciales ou des produits différents peuvent avoir des objectifs et des processus complètement différents. Avec plusieurs Comptes AWS, vous pouvez répondre aux besoins spécifiques d'une unité commerciale.
- Facturation — Un compte est le seul véritable moyen de séparer les éléments au niveau de la facturation. Les comptes multiples permettent de séparer les articles au niveau de la facturation entre les unités commerciales, les équipes fonctionnelles ou les utilisateurs individuels. Vous pouvez toujours regrouper toutes vos factures auprès d'un seul payeur (en utilisant AWS Organizations et en consolidant la facturation) tout en séparant les articles par Compte AWS.
- Allocation de quotas : les quotas AWS de service sont appliqués séparément pour chacun d'entre eux Compte AWS. La séparation des charges de travail en différentes les Comptes AWS empêche de consommer des quotas les unes pour les autres.

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

Gestion de plusieurs Comptes AWS

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

AWS propose également AWS Control Tower, qui ajoute des couches d'automatisation AWS gérée aux Organizations et l'intègre automatiquement à d'autres AWS services tels qu'Amazon AWS

CloudTrail AWS Config CloudWatch AWS Service Catalog, etc. Ces services peuvent entraîner des frais supplémentaires. Pour en savoir plus, consultez Pricing AWS Control Tower (Tarification).

Consultez aussi

- Quand utiliser AWS Organizations
- Quand utiliser AWS Control Tower

Quand utiliser AWS Organizations

AWS Organizations est 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 traitées 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 AWS Organizations, consultez le guide de AWS Organizations l'utilisateur.

Accès sécurisé

Lorsque vous gérez AWS Organizations vos comptes en tant que groupe, la plupart des tâches administratives de l'organisation ne peuvent être effectuées que 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 Organizations 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 l'accès sécurisé pour la gestion des comptes, le service de gestion des comptes autorise Organizations et son compte de gestion à accéder aux métadonnées, telles que les coordonnées principales ou secondaires, pour tous les comptes membres de l'organisation.

Pour de plus amples informations, veuillez consulter Permettre un accès fiable 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 membres comme compte administrateur délégué pour la gestion des AWS 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 ne peut accéder qu'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 de plus amples informations, veuillez consulter Activer un compte administrateur délégué pour la gestion des AWS comptes.

Politiques de contrôle des services

Lorsque vous faites Compte AWS partie d'une organisation gérée par AWS Organizations, l'administrateur de l'organisation peut appliquer des politiques de contrôle des services (SCPs) 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 membre. Un utilisateur ou un rôle (un principal) dans un compte membre ne peut effectuer que les opérations qui se situent à l'intersection de ce SCPs qui est autorisé par les règles applicables au compte et des politiques d'autorisation IAM associées au principal. Par exemple, vous pouvez l'utiliser SCPs pour empêcher le principal d'un compte de modifier les contacts alternatifs de son propre compte.

Par exemple, SCPs qui s'appliquent à Comptes AWS, voirLimitez l'accès à l'aide AWS Organizations de politiques de contrôle des services.

Permettre un accès fiable pour la gestion des AWS comptes

L'activation d'un accès sécurisé pour AWS la gestion des 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 membre dans AWS Organizations. Pour plus d'informations, consultez la section Gestion des AWS comptes et AWS Organizations le Guide de AWS Organizations l'utilisateur. Pour obtenir 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 des comptes 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 de plus amples informations, veuillez consulter Activer un compte administrateur délégué pour la gestion des AWS comptes.

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

Autorisations minimales

Pour effectuer ces tâches, vous devez satisfaire aux exigences 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 permettre un accès fiable pour la gestion des AWS comptes

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, endosser 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 de 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 enable pour le confirmer, puis choisissez Activer l'accès sécurisé.

AWS CLI & SDKs

Pour permettre un accès fiable 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 dans 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.

Activer un compte administrateur délégué pour la gestion des AWS comptes

Vous activez un compte d'administrateur délégué afin de pouvoir appeler les opérations de l'API de gestion des AWS comptes pour les autres comptes membres AWS Organizations. Une fois que vous avez enregistré un compte d'administrateur délégué pour votre organisation, les utilisateurs et les rôles de ce compte peuvent appeler les AWS CLI opérations du AWS SDK dans l'`account`espace de noms qui peuvent fonctionner en mode Organizations en prenant en charge un paramètre facultatif`AccountId`.

Pour enregistrer un compte membre dans votre organisation en tant que compte administrateur délégué, suivez la procédure suivante.

AWS CLI & SDKs

Pour enregistrer un compte d'administrateur délégué pour le service de gestion des comptes

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

> **Autorisations minimales**
>
> Pour effectuer ces tâches, vous devez satisfaire aux exigences 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 avoir activé l'accès sécurisé pour la gestion des comptes dans votre organisation.

Vous devez spécifier le principal de service suivant :

```
account.amazonaws.com
```

- AWS CLI: register-delegated-administrator

L'exemple suivant enregistre un compte membre de l'organisation en tant qu'administrateur délégué pour le service de 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 la gestion des comptes AWS CLI et les opérations API du SDK qui utilisent le `--account-id` paramètre pour référencer les comptes des membres d'une organisation.

AWS Management Console

Cette tâche n'est pas prise en charge dans la console de gestion de AWS compte. Vous ne pouvez effectuer cette tâche qu'en utilisant le AWS CLI ou une opération d'API provenant de l'un des AWS SDKs.

Limitez l'accès à l'aide AWS Organizations de politiques de contrôle des services

Cette rubrique présente des exemples qui montrent comment vous pouvez utiliser les politiques de contrôle des services (SCPs) AWS Organizations pour restreindre les actions des utilisateurs et des rôles dans les comptes de votre organisation. Pour plus d'informations sur les politiques de contrôle des services, consultez les rubriques suivantes du Guide de AWS Organizations l'utilisateur :

- Création SCPs
- Rattachement SCPs à des comptes OUs et à des comptes
- Stratégies pour SCPs
- Syntaxe de la politique SCP

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

L'exemple suivant empêche les opérations `PutAlternateContact` et `DeleteAlternateContact` API d'être appelées par un compte membre en mode compte autonome. Cela empêche les principaux titulaires des comptes concernés de modifier leurs 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 un compte membre de modifier les contacts alternatifs pour tout autre compte membre de l'organisation

L'exemple suivant généralise l'`Resource`élément en « * », ce qui signifie qu'il s'applique à la fois aux demandes en mode autonome et aux demandes en mode organisations. Cela signifie que même le compte administrateur délégué pour la gestion des comptes, si le SCP s'y applique, 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 alternatifs

L'exemple de SCP suivant inclut une condition qui compare le chemin d'organisation du compte à une liste de deux OUs. Cela empêche le principal de n'importe quel compte indiqué OUs 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/"
                    ]
                }
            }
    ]
}
```

Quand utiliser AWS Control Tower

AWS Organizations est le service de base qui vous permet de gérer et de sécuriser de manière centralisée AWS l'ensemble de votre environnement. Un élément crucial de cette approche AWS Organizations centrée est AWS Control Tower. AWS Control Tower agit comme une console de gestion au sein des Organizations, fournissant un moyen rationalisé de configurer et de gérer un AWS environnement multi-comptes sécurisé en appliquant les meilleures pratiques prescriptives.

Cette approche des meilleures pratiques de sécurité fournie par AWS Control Tower étend les fonctionnalités de base de AWS Organizations. AWS Control Tower applique un ensemble de garde-

fous préventifs et de détection pour garantir que votre organisation et vos comptes restent conformes aux normes de sécurité et de conformité recommandées.

En établissant une AWS Organizations structure bien architecturée AWS Control Tower, vous pouvez rapidement déployer un environnement évolutif, sécurisé et conforme AWS . Cette approche centralisée de la gestion et de la gouvernance du cloud est essentielle pour les entreprises qui cherchent à exploiter toute la puissance du cloud AWS Cloud tout en respectant les normes de sécurité et de conformité les plus strictes.

Pour plus d'informations, consultez Présentation de AWS Control Tower dans le Guide de l'utilisateur AWS Control Tower .

Comprendre les modes de fonctionnement des API

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

- Contexte autonome : ce mode est utilisé lorsqu'un utilisateur ou un rôle dans un compte accède ou modifie un attribut de compte dans le même compte. Le mode contextuel autonome est automatiquement utilisé lorsque vous n'incluez pas le `AccountId` paramètre lorsque vous appelez l'une des opérations de gestion de compte AWS CLI ou du AWS SDK.
- Contexte des organisations : ce mode est utilisé lorsqu'un utilisateur ou un rôle dans un compte d'une organisation accède ou modifie un attribut de compte dans un autre compte membre de la même organisation. Le mode contextuel de l'organisation est automatiquement utilisé lorsque vous incluez le `AccountId` paramètre lorsque vous appelez l'une des opérations de gestion des comptes AWS CLI ou du AWS SDK. Dans ce mode, vous pouvez appeler les opérations uniquement à partir du compte de gestion de l'organisation ou du compte administrateur délégué pour la gestion des comptes.

Les opérations du AWS SDK AWS CLI et du SDK peuvent fonctionner de manière autonome ou dans le contexte d'une organisation.

- Si vous n'incluez pas le `AccountId` paramètre, 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 d'une organisation ou non.
- Si vous incluez le `AccountId` paramètre, l'opération s'exécute dans le contexte des organisations et fonctionne sur le compte Organizations spécifié.

  - Si le compte appelant l'opération est le compte de gestion ou le compte administrateur délégué du service de gestion des comptes, vous pouvez spécifier n'importe quel compte membre de cette organisation dans le `AccountId` paramètre pour mettre à jour le compte spécifié.
  - Le seul compte d'une organisation qui peut appeler l'une des opérations de contact alternatives et spécifier son propre numéro de compte dans le `AccountId` paramètre est le compte spécifié comme compte d'administrateur délégué pour le service de gestion des comptes. Tout autre compte, y compris le compte de gestion, bénéficie d'une `AccessDenied` exception.
- Si vous exécutez une opération en mode autonome, vous devez être autorisé à exécuter l'opération avec une politique IAM incluant un `Resource` élément permettant d'`"*"`autoriser toutes les ressources ou un ARN utilisant la syntaxe d'un compte autonome.
- Si vous exécutez une opération en mode organisations, vous devez être autorisé à exécuter l'opération avec une politique IAM incluant un `Resource` élément permettant d'`"*"`autoriser toutes les ressources ou un ARN utilisant la syntaxe d'un compte de membre dans une organisation.

Octroi d'autorisations pour mettre à jour les attributs du compte

Comme pour la plupart des AWS opérations, vous accordez des autorisations pour ajouter, mettre à jour ou supprimer des attributs de compte Comptes AWS en utilisant les politiques d'autorisation IAM. Lorsque vous associez une politique d'autorisation IAM à un principal IAM (utilisateur ou rôle), vous spécifiez les actions que ce principal peut effectuer sur quelles ressources et dans quelles conditions.

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

Format du nom de ressource Amazon pour Comptes AWS

- Le nom de ressource Amazon (ARN) d'un compte Compte AWS que vous pouvez inclure dans l'`resource`élément d'une déclaration de politique 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 des 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'attribution de compte en mode autonome en n'incluant pas le `AccountID` paramètre.

- Un ARN de compte pour le compte d'un membre d'une organisation :

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

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

Clés de contexte pour les politiques IAM

Le service de gestion des comptes fournit également plusieurs clés de condition spécifiques au service de gestion des comptes qui permettent de contrôler avec précision les autorisations que vous accordez.

`account:AccountResourceOrgPaths`

La clé de contexte vous `account:AccountResourceOrgPaths` permet de définir un chemin à travers la hiérarchie de votre organisation vers une unité organisationnelle (UO) spécifique. Seuls les comptes de membres contenus dans cette unité d'organisation répondent à cette condition. L'exemple d'extrait suivant limite l'application de la politique aux seuls comptes figurant dans l'un des deux comptes spécifiés. OUs

Comme il `account:AccountResourceOrgPaths` s'agit d'un type de chaîne à valeurs multiples, vous devez utiliser les opérateurs de chaîne `ForAnyValue` ou `ForAllValues` à valeurs multiples. Notez également que le préfixe de la clé de condition est`account`, même si vous faites référence à des chemins OUs dans 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 de contexte vous `account:AccountResourceOrgTags` 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 classer et étiqueter les ressources de votre compte. Pour plus d'informations sur le balisage, consultez la section Éditeur de balises dans le guide de l'AWS Resource Groups utilisateur. Pour plus d'informations sur l'utilisation des balises dans le cadre d'une stratégie de contrôle d'accès basée sur les attributs, voir À quoi sert ABAC AWS dans le guide de l'utilisateur IAM. L'exemple d'extrait suivant limite l'application de la politique aux seuls comptes d'une organisation dont la balise comporte la clé `project` et la valeur de ou. `blue` `red`

Comme il `account:AccountResourceOrgTags` s'agit d'un type de chaîne à valeurs multiples, vous devez utiliser les opérateurs de chaîne `ForAnyValue` ou `ForAllValues` 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 tags qu'à un seul compte d'une organisation. Vous ne pouvez pas associer de balises à un appareil autonome. Compte AWS

Configurez votre Compte AWS

Cette section inclut des rubriques qui décrivent comment gérer votre Compte AWS.

> **Note**
>
> Si vous avez Compte AWS été créé en Inde à l'aide d'Amazon Web Services India Private Limited (AWS Inde), d'autres considérations doivent être prises en compte. Pour de plus amples informations, veuillez consulter Gérer des comptes en Inde.

Rubriques

Création d'un 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 AWS ID, vous pouvez créer un alias de compte.

Pour savoir comment créer ou mettre à jour un alias de compte, consultez la section Utilisation d'un alias pour votre Compte AWS identifiant dans le guide de l'utilisateur IAM.

Activez ou désactivez Régions AWS dans votre compte

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, consultez la section 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 EC2 instances Amazon 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 de plus amples informations, veuillez consulter 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, voir 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 pour 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 activées par défaut.

Nom	Code
USA Est (Virginie du Nord)	`us-east-1`
USA Est (Ohio)	`us-east-2`
USA Ouest (Californie du Nord)	`us-west-1`
USA Ouest (Oregon)	`us-west-2`

Nom	Code
Asie Pacifique (Tokyo)	`ap-northeast-1`
Asie-Pacifique (Séoul)	`ap-northeast-2`
Asie-Pacifique (Osaka)	`ap-northeast-3`
Asie-Pacifique (Mumbai)	`ap-south-1`
Asie-Pacifique (Singapour)	`ap-southeast-1`
Asie-Pacifique (Sydney)	`ap-southeast-2`
Canada (Centre)	`ca-central-1`
Europe (Francfort)	`eu-central-1`
Europe (Stockholm)	`eu-north-1`
Europe (Irlande)	`eu-west-1`
Europe (Londres)	`eu-west-2`
Europe (Paris)	`eu-west-3`
Amérique du Sud (São Paulo)	`sa-east-1`

- Vous pouvez utiliser toutes les régions de destination dans une zone d'inférence interrégionale, quel que soit le statut de région choisie. Certains services d'IA AWS générative, notamment Amazon Bedrock (voir Augmenter le débit grâce à l'inférence interrégionale) et Amazon Q Developer (voir Traitement interrégional dans Amazon Q Developer) utilisent l'inférence entre régions. Si vous utilisez ces services, ils sélectionnent automatiquement les options optimales, Région AWS y compris les régions que vous n'avez pas activées pour les ressources et les données IAM, dans la zone géographique que vous avez choisie. Cela améliore l'expérience client en maximisant le calcul disponible et la disponibilité des modèles.
- 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, comme 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 EC2 instance 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 EC2 instances Amazon, vous devez toujours payer les frais associés à 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 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 à la gestion des AWS comptes APIs 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 fiable 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 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 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"
  }
```

Mettez à jour la facturation de votre Compte AWS

Vous pouvez mettre à jour toutes vos préférences de Compte AWS facturation à l'aide de la console AWS Billing and Cost Management. Pour savoir comment mettre à jour les paramètres de facturation de votre compte, consultez le guide de l'AWS Billing and Cost Management utilisateur :

Mettre à jour l'adresse e-mail de l'utilisateur root (adresse)

Il existe plusieurs raisons professionnelles pour lesquelles vous devrez peut-être mettre à jour l'adresse e-mail de l'utilisateur root (adresse) de votre Compte AWS. Par exemple, la sécurité et la résilience administrative. Cette rubrique explique le processus de mise à jour de votre adresse e-mail utilisateur root (adresse e-mail) pour les comptes autonomes et les comptes membres.

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

Vous pouvez mettre à jour l'e-mail de l'utilisateur root () 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 l'e-mail de l'utilisateur root (e-mail) à l'aide de la console AWS de gestion. Pour savoir comment procéder, consultez Mettre à jour l'adresse e-mail de l'utilisateur root pour une version autonome. Compte AWS
- 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 l'e-mail de l'utilisateur root () du compte membre depuis la AWS Organizations console ou par programmation via la AWS CLI &. SDKs Pour savoir comment procéder, consultez Mettre à jour l'adresse e-mail de l'utilisateur root pour tous les Compte AWS membres de votre organisation.

Rubriques

Mettre à jour l'adresse e-mail de l'utilisateur root () pour une version autonome Compte AWS

Pour modifier l'adresse e-mail de l'utilisateur root (adresse) pour un appareil autonome Compte AWS, suivez les étapes de la procédure suivante.

AWS Management Console

> **Note**
>
> 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 Détails du compte, choisissez Actions, puis sélectionnez Mettre à jour l'adresse e-mail et le mot de passe.
4. Sur la page Détails du compte, à côté de Adresse e-mail, choisissez Modifier.
5. Sur la page Modifier l'adresse e-mail du compte, remplissez les champs Nouvelle adresse e-mail, Confirmez la nouvelle adresse e-mail et confirmez votre mot de passe actuel. Choisissez ensuite Enregistrer et continuer. Un code de vérification est envoyé à votre nouvelle adresse e-mail depuis`no-reply@verify.signin.aws`.
6. Sur la page Modifier l'adresse e-mail du compte, sous Code de vérification, entrez le code que vous avez reçu par e-mail, puis choisissez Confirmer les mises à jour.

> **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.

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 SDKs. Vous ne pouvez effectuer cette tâche qu'à l'aide du AWS Management Console.

Mettez à jour l'adresse e-mail de l'utilisateur root (e-mail) pour n'importe quel Compte AWS membre de votre organisation

Pour modifier l'adresse e-mail de l'utilisateur root (adresse) pour n'importe quel compte membre de votre organisation à l'aide de la AWS Organizations console, effectuez les étapes de la procédure suivante.

> **Note**
>
> Avant de mettre à jour l'adresse e-mail de l'utilisateur root () pour un compte membre, nous vous recommandons de comprendre l'impact de cette opération. Pour plus d'informations, consultez la section Mise à jour de l'adresse e-mail de l'utilisateur root () pour un compte membre AWS Organizations dans le Guide de AWS Organizations l'utilisateur.

Vous pouvez également mettre à jour l'adresse e-mail de l'utilisateur root () d'un compte membre directement depuis la page Compte AWS Management Console après vous être connecté en tant qu'utilisateur root. Pour step-by-step obtenir des instructions, suivez les étapes indiquées dansMettre à jour l'adresse e-mail de l'utilisateur root () pour une version autonome Compte AWS.

AWS Management Console

> **Remarques**
>
> - Pour exécuter cette procédure à partir du compte de gestion ou d'un compte administrateur délégué d'une organisation par rapport aux comptes des membres, vous devez activer l'accès sécurisé pour le service de gestion des comptes.
> - Vous ne pouvez pas utiliser cette procédure pour accéder à un compte appartenant à une autre organisation que celle que vous utilisez pour appeler l'opération.

Pour mettre à jour l'adresse e-mail de l'utilisateur root (adresse) d'un compte membre à l'aide de la AWS Organizations console

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM ou en tant qu'utilisateur root (ce n'est pas recommandé) dans le compte de gestion de l'organisation.
2. Sur la Comptes AWSpage, choisissez le compte membre pour lequel vous souhaitez mettre à jour l'adresse e-mail de l'utilisateur root (adresse e-mail).
3. Dans la section Détails du compte, cliquez sur le bouton Actions, puis sélectionnez Mettre à jour l'adresse e-mail.
4. Sous E-mail, entrez la nouvelle adresse e-mail de l'utilisateur root, puis choisissez Enregistrer. Cela envoie un mot de passe à usage unique (OTP) à la nouvelle adresse e-mail.

> **Note**
>
> Si vous devez fermer cette page dans la console Organizations pendant que vous attendez le code, vous pouvez revenir et terminer le processus OTP dans les 24 heures suivant l'envoi du code. Pour ce faire, sur la page des détails du compte, cliquez sur le bouton Actions, puis sur Terminer la mise à jour par e-mail.

5. Sous Code de vérification, entrez le code envoyé à la nouvelle adresse e-mail à l'étape précédente, puis choisissez Confirmer. La mise à jour du compte est alors validée pour l'utilisateur root.

AWS CLI & SDKs

Vous pouvez récupérer ou mettre à jour l'adresse e-mail de l'utilisateur root (également appelée adresse e-mail principale) à l'aide des AWS CLI commandes suivantes ou de leurs opérations équivalentes dans le AWS SDK :

- GetPrimaryEmail
- StartPrimaryEmailUpdate
- AcceptPrimaryEmailUpdate

> **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 de gestion des comptes.
> - 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:GetPrimaryEmail`
> - `account:StartPrimaryEmailUpdate`
> - `account:AcceptPrimaryEmailUpdate`
>
> Si vous utilisez ces autorisations individuelles, vous pouvez autoriser certains utilisateurs à lire uniquement l'adresse e-mail de l'utilisateur root (), tandis que d'autres peuvent lire et écrire.

Pour terminer le processus d'adresse e-mail de l'utilisateur root , vous devez utiliser l'e-mail principal APIs ensemble dans l'ordre indiqué dans les exemples ci-dessous.

Example **`GetPrimaryEmail`**

L'exemple suivant extrait l'adresse e-mail de l'utilisateur root (adresse e-mail) à partir du 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-primary-email --account-id 123456789012
```

Example **`StartPrimaryEmailUpdate`**

L'exemple suivant lance le processus de mise à jour de l'adresse e-mail de l'utilisateur root , identifie la nouvelle adresse e-mail et envoie un mot de passe à usage unique (OTP) à la nouvelle adresse e-mail 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.

```
$ aws account start-primary-email-update --account-id 123456789012 --primary-email
 john@examplecorp.com
```

Example **`AcceptPrimaryEmailUpdate`**

L'exemple suivant accepte le code OTP et attribue à la nouvelle adresse e-mail 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 accept-primary-email-update --account-id 123456789012 --otp 12345678
 --primary-email john@examplecorp.com
```

Mettre à jour le mot de passe utilisateur root

Pour modifier le mot Compte AWS de passe de votre utilisateur root, suivez les étapes de la procédure suivante.

AWS Management Console

Pour modifier le mot de passe de votre utilisateur root

> **Note**
>
> 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 Détails du compte, choisissez Actions, puis sélectionnez Mettre à jour l'adresse e-mail et le mot de passe.
4. Sur la page Détails du compte, à côté de Mot de passe, choisissez Modifier.
5. Sur la page Modifier le mot de passe, renseignez les champs Mot de passe actuel, Nouveau mot de passe et Confirmer le nouveau mot de passe. Choisissez ensuite Mettre à jour le mot de passe. 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.

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 SDKs. Vous ne pouvez effectuer cette tâche qu'à l'aide du AWS Management Console.

Mettez à jour votre Compte AWS nom

Lorsque vous en gérez plusieurs Comptes AWS, utilisez des conventions de dénomination claires alignées sur les unités commerciales et les applications pour l'identification et l'organisation. Lors de réorganisations, de fusions, d'acquisitions ou de mises à jour de conventions de dénomination, il se peut que vous deviez renommer les comptes afin de maintenir des normes d'identification et administratives cohérentes.

Le nom d'un 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 qu'ils soient faciles à reconnaître. Pour les comptes d'entreprise, pensez à utiliser une norme de dénomination telle que organisation - objectif - environnement (par exemple, ventes - catalogue - production). Pour des raisons de confidentialité et de sécurité, évitez d'utiliser des noms de compte qui reflètent des informations personnelles identifiables (PII).

- Autonome Comptes AWS : si vous n'êtes Comptes AWS pas associé à une organisation, vous pouvez mettre à jour le nom de votre compte en utilisant le AWS Management Console, ou le AWS CLI et SDKs. Pour savoir comment procéder, consultez Mettez à jour le nom de votre compte pour un compte autonome Compte AWS.
- Comptes AWS au sein d'une organisation : pour les comptes membres faisant partie d'une AWS Organizations, un utilisateur du compte de gestion ou du compte administrateur délégué peut mettre à jour de manière centralisée le nom de compte de n'importe quel compte membre de l'organisation depuis la AWS Organizations console ou par programmation via le AWS CLI et. SDKs Pour savoir comment procéder, consultez Mettez à jour le nom de votre compte pour n'importe quel Compte AWS membre de votre organisation.

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

Rubriques

Mettez à jour le nom de votre compte pour un compte autonome Compte AWS

Pour modifier le nom du compte d'un compte autonome Compte AWS, suivez les étapes de la procédure suivante.

AWS Management Console

> **Autorisations minimales**
>
> Vous pouvez mettre à jour le nom de votre compte à l'aide de l'utilisateur root, d'un utilisateur IAM ou d'un rôle IAM. Si vous utilisez l'utilisateur root, aucune autorisation IAM supplémentaire n'est nécessaire pour mettre à jour le nom d'un compte. Lorsque vous utilisez un utilisateur ou un rôle IAM, vous devez disposer au moins des autorisations IAM suivantes :
>
> - `account:GetAccountInformation`
> - `account:PutAccountName`

Pour mettre à jour le nom du compte d'un compte autonome

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 Détails du compte, choisissez Actions, puis sélectionnez Mettre à jour le nom du compte.
4. Sous Nom, entrez le nouveau nom de compte que vous souhaitez mettre à jour, puis choisissez Enregistrer.

AWS CLI & SDKs

> **Autorisations minimales**
>
> Vous pouvez mettre à jour le nom de votre compte à l'aide de l'utilisateur root, d'un utilisateur IAM ou d'un rôle IAM. Pour effectuer les étapes suivantes, votre utilisateur ou rôle IAM doit disposer au moins des autorisations IAM suivantes :
>
> - `account:GetAccountInformation`
> - `account:PutAccountName`

Pour mettre à jour le nom du compte d'un compte autonome

Vous pouvez utiliser l'une des opérations suivantes :

- AWS CLI: put-account-name

```
$ C:\> aws account put-account-name \
        --account-name "New-Account-Name"
```

- AWS SDKs: PutAccountName

Mettez à jour le nom de votre compte pour n'importe quel Compte AWS membre de votre organisation

En mode AWS Organizations avec toutes les fonctionnalités, les utilisateurs IAM autorisés ou les rôles IAM dans les comptes de gestion et d'administration déléguée peuvent gérer les noms de compte de manière centralisée.

Pour modifier le nom d'un compte de membre de votre organisation, suivez les étapes de la procédure ci-dessous.

Prérequis

Pour mettre à jour le nom d'un compte avec la AWS Organizations console, vous devez effectuer certains réglages 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 pour une organisation.
- Vous devez activer l'accès sécurisé pour le service de gestion des AWS comptes. Pour configurer cela, voirPermettre un accès fiable pour la gestion des AWS comptes.

AWS Management Console

> **Autorisations minimales**
>
> Pour mettre à jour le nom d'un compte membre, votre utilisateur IAM ou votre rôle IAM doit disposer des autorisations suivantes :
>
> - `organizations:DescribeOrganization` (console uniquement)
> - `account:PutAccountName`

Pour mettre à jour le nom du compte d'un membre

1. Ouvrez la console Organizations à l'adresse https://console.aws.amazon.com/organizations/.
2. Dans le panneau de navigation de gauche, choisissez Comptes AWS.
3. Sur la Comptes AWSpage, choisissez le compte membre que vous souhaitez mettre à jour, choisissez le menu déroulant Actions, puis choisissez Mettre à jour le nom du compte.
4. Sous Nom, entrez le nom mis à jour, puis choisissez Enregistrer.

AWS CLI & SDKs

> **Autorisations minimales**
>
> Pour mettre à jour le nom d'un compte membre, votre utilisateur IAM ou votre rôle IAM doit disposer des autorisations suivantes :
>
> - `organizations:DescribeOrganization` (console uniquement)
> - `account:PutAccountName`

Pour mettre à jour le nom du compte d'un membre

Vous pouvez utiliser l'une des opérations suivantes :

- AWS CLI: put-account-name

```
$ C:\> aws account put-account-name \
        --account-id 111111111111 \
        --account-name "New-Account-Name"
```

- AWS SDKs: PutAccountName

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 de AWS gestion ou via AWS CLI & SDKs. Pour savoir comment procéder, voir Mettre à jour les contacts secondaires pour un appareil autonome. Compte AWS
- 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 &. SDKs Pour savoir comment procéder, voir Mettre à jour les contacts alternatifs de n'importe quel Compte AWS membre de 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. 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 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 pour une organisation.
- Vous devez activer l'accès sécurisé pour le service de gestion des AWS comptes. Pour configurer cela, voirPermettre un accès fiable pour la gestion des AWS comptes.

> **Note**
>
> Les politiques AWS Organizations `AWSOrganizationsReadOnlyAccess` gérées `AWSOrganizationsFullAccess` sont mises à jour pour autoriser l'accès à la gestion des AWS comptes APIs 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. 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 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 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 :

- `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 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 de AWS gestion ou via AWS CLI & SDKs. Pour savoir comment procéder, voir Mettre à jour le contact Compte AWS principal autonome.
- 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 &. SDKs 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

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 doivent contenir que des chiffres.
- 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 ne doivent pas comporter de tirets ou d'espaces « - » entre l'indicatif régional, le code d'échange et le code local. Par exemple, +12025550179.
- Pour des raisons de sécurité, les numéros de téléphone doivent pouvoir recevoir des SMS AWS. Les numéros sans frais ne seront pas acceptés car la plupart ne supportent pas les SMS.
- 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. 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 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 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 pour une organisation.
- Vous devez activer l'accès sécurisé pour le service de gestion des AWS comptes. Pour configurer cela, voirPermettre un accès fiable 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 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 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.

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 AWS De nombreuses AWS ressources incluent l'ID de compte dans leur nom de ressource Amazon (ARNs). 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 le compte IDs, comme toute information d'identification, doive être utilisé et partagé avec soin, il n'est pas considéré comme une information secrète, sensible ou confidentielle.

ID utilisateur canonique

Un identifiant alphanumérique, tel que`e79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be`, qui est une forme obfusquée 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 Amazon S3 (ACLs).

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 AWS utilisateurs IAM ou les rôles IAM.

Utilisez la commande list-buckets comme suit.

```
$ aws s3api list-buckets \
    --max-items 10 \
    --page-size 10 \
    --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. Sélectionnez l’onglet 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 AWS utilisateurs IAM ou les rôles IAM.

Utilisez la commande list-buckets comme suit.

```
$ aws s3api list-buckets \
    --max-items 10 \
    --page-size 10 \
    --query Owner.ID \
    --output text
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

Sécurité dans la gestion des AWS comptes

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

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

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à la gestion des comptes, voir Services AWS champ par programme Services AWS de conformité et .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service 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 lors de l'utilisation de la gestion des AWS comptes. Il vous explique comment configurer la gestion des comptes pour atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources de gestion de 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 chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. 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 des Services AWS que vous utilisez. Pour plus d'informations 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 AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs 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 le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent 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 par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez Norme FIPS (Federal Information Processing Standard) 140-3.

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 Nom. Cela inclut lorsque vous travaillez avec Account Management ou autre Services AWS

à l'aide de la console, de l'API ou AWS SDKs. AWS CLI Toutes les données que vous entrez 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 PrivateLink pour la gestion des AWS comptes

Si vous utilisez Amazon Virtual Private Cloud (Amazon VPC) pour héberger vos AWS ressources, vous pouvez accéder au service de gestion des AWS comptes depuis le VPC sans avoir à passer par l'Internet public.

Amazon VPC vous permet de lancer AWS des ressources dans 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 VPCs, consultez le guide de l'utilisateur Amazon VPC.

Pour connecter votre Amazon VPC à Account Management, vous devez d'abord définir un point de terminaison VPC d'interface, qui vous permet de connecter votre VPC à d'autres services. AWS 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 un point de terminaison de gestion de AWS compte dans votre VPC à l'aide du AWS Management Console, the AWS Command Line Interface (AWS CLI), d'un AWS SDK, de l'API de gestion des AWS comptes ou. AWS 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 du 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 Account Management comme le service auquel vous souhaitez que votre VPC se connecte, en utilisant le format suivant :

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

Vous devez utiliser la chaîne exactement comme indiqué, en spécifiant la `us-east-1` région. En tant que service mondial, la gestion des comptes est hébergée dans cette seule AWS région.

Pour plus d'informations sur la création et la configuration d'un point de terminaison à l'aide AWS CloudFormation de la VPCEndpoint ressource AWS EC2 : : : : dans le guide de AWS CloudFormation l'utilisateur.

Politiques relatives aux terminaux Amazon VPC

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

- Politiques relatives aux terminaux Amazon Virtual Private Cloud pour la gestion des comptes
- Contrôle de l'accès aux services avec les points de terminaison VPC dans le guide.AWS PrivateLink

Politiques relatives aux terminaux Amazon Virtual Private Cloud pour la gestion des comptes

Vous pouvez créer une politique de point de terminaison Amazon VPC pour la gestion des comptes dans laquelle vous spécifiez les éléments suivants :

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

L'exemple suivant montre une politique de point de terminaison Amazon VPC qui permet à un utilisateur IAM nommé Alice dans le compte 123456789012 de récupérer et de modifier les informations de contact alternatives pour n'importe quel compte Compte 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 souhaitez accorder l'accès aux comptes faisant partie d'une AWS organisation à un directeur qui possède l'un des comptes membres de l'organisation, l'`Resource`élément doit utiliser le format suivant :

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

Pour plus d'informations sur la création de politiques de point de terminaison, consultez la section Contrôle de l'accès aux services avec des points de terminaison VPC dans le guide.AWS PrivateLink

Identity and Access Management pour la gestion des AWS comptes

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

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

Rubriques

Public ciblé

Votre utilisation d' AWS Identity and Access Management (IAM) diffère selon la tâche que vous accomplissez dans Account Management.

Utilisateur du service — Si vous utilisez le service de gestion de compte pour effectuer votre tâche, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Plus vous utiliserez de fonctions de gestion de compte pour effectuer votre travail, plus vous pourriez avoir besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans la gestion du compte, consultezRésolution des problèmes d'identité et d'accès à la gestion des AWS comptes.

Administrateur du service — Si vous êtes le responsable des ressources de gestion des comptes de votre entreprise, vous bénéficiez probablement d'un accès total à la gestion des comptes. Votre responsabilité est de déterminer les fonctions et ressources de gestion de compte auxquelles les utilisateurs de votre 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 Account Management, veuillez consulterComment fonctionne la gestion des AWS comptes avec IAM.

Administrateur IAM — Si vous êtes un administrateur IAM, vous souhaiterez peut-être obtenir des détails sur la façon dont vous pouvez écrire des stratégies pour gérer l'accès à la gestion des comptes. Pour voir des exemples de politiques basées sur l'identité de gestion de compte que vous

pouvez utiliser dans IAM, veuillez consulter. Exemples de stratégies basées sur l'identité pour AWS la gestion des comptes

Authentification par des identités

L'authentification correspond au processus par lequel vous connectez à AWS l'aide de vos informations d'identification. Vous devez vous authentifier (être connecté à AWS) en tant qu' Utilisateur racine d'un compte AWS, en tant qu'utilisateur IAM ou en endossant un rôle IAM.

Vous pouvez vous connecter à en AWS tant qu'identité fédérée à l'aide des informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification de connexion 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 en utilisant la fédération, vous endossez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter à la 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 accédez à AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos requêtes à l'aide de vos informations d'identification. Si vous n'utilisez pas AWS les outils, vous devez signer les requêtes vous-même. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer des demandes vous-même, consultez AWS Signature Version 4 pour les demandes 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, vous AWS recommande d'utiliser la Multi-Factor Authentication (MFA) pour améliorer la sécurité de votre compte. Pour plus d'informations, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Authentification multifactorielle AWS dans IAM dans le Guide de l'utilisateur IAM.

Compte AWS Utilisateur racine

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 l'utilisateur Compte AWS racine du. Vous pouvez y accéder en vous connectant à

l'aide de l'adresse e-mail et du mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur racine, consultez Tâches nécessitant des informations d'identification d'utilisateur racine dans le Guide de l'utilisateur IAM.

Identité fédérée

Demandez aux utilisateurs humains, et notamment aux utilisateurs qui nécessitent un accès administrateur, d'appliquer la bonne pratique consistant à utiliser une fédération avec fournisseur d'identité pour accéder à en Services AWS utilisant des informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, un fournisseur d'identité Web, l' AWS Directory Service, l'annuaire Identity Center ou tout utilisateur qui accède à en Services AWS utilisant des informations d'identification fournies via une source d'identité. Lorsque des identités fédérées accèdent à Comptes AWS, elles assument des rôles, ces derniers fournissant 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 connecter et vous synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité pour une utilisation sur l'ensemble de vos applications Comptes AWS et de vos. 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 dans votre Compte AWS qui dispose d'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 telles que des mots de passe et des 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 d'effectuer une rotation des 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 IAMAdminset accorder à ce groupe les autorisations leur permettant 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 plus d'informations, consultez Cas d'utilisation pour les utilisateurs IAM 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. Pour endosser temporairement un rôle IAM dans la AWS Management Console, vous pouvez passer d'un rôle utilisateur à un rôle IAM (console). Vous pouvez endosser un rôle en appelant une opération d' AWS API AWS CLI ou à l'aide d'une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Méthodes pour endosser un rôle 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 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 Services AWS, certains vous permettent d'attacher une stratégie directement à une ressource (au lieu d'utiliser un rôle en tant

que proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

- Accès services multiples — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant pour ce service d'exécuter des applications dans Amazon EC2 ou de stocker 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.
  - Transmission de sessions d'accès (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions dans AWS, vous êtes considéré comme un principal. 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 qui appelle Service AWS, combinées Service AWS à qui demande pour effectuer des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande dont l'exécution nécessite des interactions avec d'autres Services AWS ou ressources. 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.
  - 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 un rôle de 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 s'affichent dans votre Compte AWS et sont détenus par le service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.
- Applications s'exécutant sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer des informations d'identification temporaires pour les applications s'exécutant sur une EC2 instance et effectuant des requêtes d' AWS API AWS CLI ou. Cette solution est préférable au stockage des clés d'accès au sein de l' EC2 instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible à toutes les applications associées, vous pouvez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l' EC2 instance d'obtenir des informations d'identification temporaires. Pour de plus amples informations, veuillez consulter Utiliser un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des EC2 instances Amazon dans le Guide de l'utilisateur IAM.

Gestion des accès à l’aide de politiques

Vous contrôlez les accès dans en AWS créant des stratégies et en les attachant à AWS des identités ou à des ressources. Une stratégie est un objet dans AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit les autorisations de ces dernières. AWS évalue ces stratégies lorsqu'un principal (utilisateur, utilisateur racine ou session de rôle) envoie une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des stratégies sont stockées dans en AWS tant que 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 stratégies 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 Définition d’autorisations IAM personnalisées avec des politiques gérées par le client 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 stratégies gérées sont des stratégies autonomes que vous pouvez lier à plusieurs utilisateurs, groupes et rôles de votre Compte AWS. Les stratégies gérées incluent des stratégies AWS gérées par et des stratégies 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. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. 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, utilisateurs, utilisateurs, rôles, utilisateurs fédérés ou des. Services AWS

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

Listes de contrôle d'accès (ACLs)

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

Amazon S3 AWS WAF, et Amazon VPC sont des exemples de services qui sont compatibles. ACLs Pour en savoir plus ACLs, consultez Présentation 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 stratégies moins courantes. 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 annule 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 de service (SCPs) : SCPs sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité d'organisation (UO) dans AWS Organizations. AWS Organizations est un service permettant de regrouper et de gérer de façon centralisée plusieurs Comptes AWS détenus par votre entreprise. Si vous activez toutes les fonctions d'une organisation, vous pouvez appliquer les stratégies de contrôle de service (SCPs) à l'un ou à l'ensemble de vos comptes. La SCP limite les autorisations pour les entités dans les comptes membres, y compris dans chaque Utilisateur racine d'un compte AWS. Pour plus d'informations sur les Organizations et consultez SCPs les politiques de contrôle des services dans le Guide de AWS Organizations l'utilisateur.
- Politiques de contrôle des ressources (RCPs) : RCPs sont des politiques JSON que vous pouvez utiliser pour définir le nombre maximum d'autorisations disponibles pour les ressources de vos comptes sans mettre à jour les politiques IAM associées à chaque ressource que vous possédez. Le RCP limite les autorisations pour les ressources des comptes membres et peut avoir un impact sur les autorisations effectives pour les identités, y compris le Utilisateur racine d'un compte AWS, qu'elles appartiennent ou non à votre organisation. Pour plus d'informations sur les Organizations RCPs, y compris une liste de ces Services AWS supports RCPs, consultez la section Resource control policies (RCPs) dans le guide de AWS Organizations l'utilisateur.
- 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 session 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 découvrir la façon dont AWS détermine s'il convient d'autoriser une demande en présence de plusieurs types de stratégies, consultez Logique d'évaluation de stratégies 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 de compte, découvrez les fonctions IAM que vous pouvez utiliser avec.

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

Fonctionnalité 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 de politique	Oui
ACLs	Non
ABAC (étiquettes dans les politiques)	Non
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 d'autres AWS services fonctionnent avec la plupart des fonctions d'IAM, consultez AWS services that work with IAM (Services qui fonctionnent avec IAM) dans le Guide de l'utilisateur IAM.

Stratégies 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 Définition d'autorisations IAM personnalisées avec des politiques gérées par le client 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 stratégies basées sur l'identité pour la gestion des comptes

Pour voir des exemples de stratégies basées sur l'identité dans la gestion des comptes, consultez. Exemples de stratégies basées sur l'identité pour AWS la gestion des comptes

Politiques basées sur une ressource dans 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. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. 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, utilisateurs, utilisateurs, rôles, utilisateurs fédérés ou des. 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 intercompte 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 se trouvent dans des différents Comptes AWS, un administrateur IAM dans le compte approuvé doit également accorder

à l'entité principal (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 Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Actions politiques pour la gestion des comptes

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser les stratégies 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 possèdent 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 politique 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 stratégie dans Account Management commencent par 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 autres contacts Compte AWS d'un, incluez l'action suivante.

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

Pour voir des exemples de stratégies basées sur l'identité dans la gestion des comptes, consultez. Exemples de stratégies 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 stratégies 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 caractéristiques ARNs, consultez la section Ressources définies par la gestion des AWS comptes dans la référence d'autorisation de service. Pour savoir grâce à quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par AWS Account Management.

Pour voir des exemples de stratégies basées sur l'identité dans la gestion des comptes, consultez. Exemples de stratégies basées sur l'identité pour AWS la gestion des comptes

Clés de condition de stratégie pour la gestion des comptes

Prend en charge les clés de condition de politique spécifiques au service : oui

Les administrateurs peuvent utiliser les stratégies 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 à un service. Pour afficher toutes les clés de condition AWS globales, consultez 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 fournir un filtrage précis pour vos stratégies 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 de chemins à travers la hiérarchie de votre organisation vers des unités organisationnelles (UO) spécifiques. Il vous permet de filtrer la politique pour qu'elle n'affecte que les comptes cibles d'une unité d'organisation correspondante.

  ```
  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 afficher la liste des clés de condition de gestion de compte, veuillez consulter Clés de condition pour la gestion de AWS compte dans la Référence de l'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez Actions définies par la gestion de AWS compte.

Pour voir des exemples de stratégies basées sur l'identité dans la gestion des comptes, consultez. Exemples de stratégies basées sur l'identité pour AWS la gestion des comptes

Listes de contrôle d'accès dans la gestion des comptes

Supports ACLs : Non

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

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

Prend en charge ABAC (identifications dans les politiques) : Non

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 attacher des balises à des entités IAM (utilisateurs ou rôles), ainsi qu'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 la gestion des AWS comptes, le contrôle d'accès basé sur des balises n'est pris en charge que par le biais de la clé de `account:AccountResourceOrgTags/key-name` condition. La clé de `aws:ResourceTag/key-name` condition standard n'est pas prise en charge APIs dans l'espace de noms du compte.

Exemple de politique JSON utilisant la clé de condition prise en charge

L'exemple de politique suivant permet d'accéder aux informations de contact des comptes marqués avec la clé « » CostCenter et la valeur « 12345 » ou « 67890 » dans votre organisation.

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

```
         "Action":[
            "account:GetContactInformation",
            "account:GetAlternateContact"
         ],
         "Resource":"*",
         "Condition":{
            "ForAnyValue:StringEquals":{
               "account:AccountResourceOrgTags/CostCenter":[
                  "12345",
                  "67890"
               ]
            }
         }
      }
   ]
}
```

Pour plus d'informations sur ABAC, voir Définir les autorisations en fonction des attributs avec l'autorisation ABAC et didacticiel IAM : Définir les autorisations d'accès aux AWS ressources en fonction des balises dans le guide de l'utilisateur IAM.

Utilisation des informations d'identification temporaires avec Account Management

Prend en charge les informations d’identification temporaires : oui

Certains Services AWS ne fonctionnent pas quand vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, notamment sur les qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS qui fonctionnent avec IAM dans le Guide de l'utilisateur IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à la en AWS Management Console utilisant toute méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS en utilisant le lien d'authentification unique (SSO) de votre société, 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 Passage d’un rôle utilisateur à un rôle IAM (console) dans le Guide de l’utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS CLI ou de AWS l'API. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y

accéder AWS. AWS vous recommande de générer des informations d'identification temporaires de façon dynamique 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 entre services pour la gestion des comptes

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

Lorsque vous vous servez d'un utilisateur ou d'un rôle IAM pour accomplir des actions dans AWS, vous êtes considéré comme un principal. 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 qui appelle Service AWS, combinées Service AWS à qui demande pour effectuer des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande dont l'exécution nécessite des interactions avec d'autres Services AWS ou ressources. 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 rôles de service : Non

Un rôle de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de 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 à un service 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 s'affichent dans votre Compte AWS et sont détenus par le 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 stratégies basées sur l'identité pour AWS la gestion des comptes

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou modifier les 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 IAM (console) dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par Account Management, notamment le format du ARNs pour chaque type de ressource, consultez Actions, ressources et clés de condition pour la gestion des AWS comptes dans la Référence de l'autorisation de service.

Rubriques

Bonnes pratiques en matière de politiques

Les stratégies basées sur l'identité déterminent si une personne peut créer, consulter 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 :

- Démarrez avec les politiques AWS gérées et évoluez vers les autorisations de moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et charges de travail, utilisez les politiques AWS gérées par qui accordent des autorisations dans de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire encore les autorisations en définissant des stratégies gérées par le AWS client qui sont propres 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.

- Accordez 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 d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utilisez 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 via un spécifique Service AWS, comme AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM 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 politiques avec IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Authentification multifactorielle (MFA) nécessaire. - Si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur racine dans Compte AWS votre, activez l'authentification multifactorielle pour plus de sécurité. Pour exiger la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec 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 informations relatives à 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 vous assurer que les utilisateurs et les rôles puissent utiliser la console de gestion des comptes, vous pouvez choisir d'associer la stratégie `AWSAccountManagementReadOnlyAccess` ou la stratégie `AWSAccountManagementFullAccess` AWS gérée aux entités. Pour plus d'informations, consultez Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

Vous n'avez pas besoin d'accorder les autorisations minimales de console aux utilisateurs qui n'effectuent des appels qu'à l' AWS interface de ligne de commande ou l' AWS API. Dans de nombreux cas, vous pouvez choisir d'accorder l'accès à uniquement aux actions qui correspondent aux opérations d'API que vous tentez d'effectuer.

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

Dans l'exemple suivant, vous souhaitez accorder à un utilisateur IAM dans votre 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 permet d'accéder 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 des stratégies basées sur l'identité (stratégies IAM) pour la gestion des comptes AWS

Pour une présentation complète des utilisateurs IAM, consultez Comptes AWS What IAM ? (Qu'est-ce qu'IAM ?) dans 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 (Modification des stratégies IAM) 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 obtenir des exemples de stratégies qui utilisent ces autorisations, consultez Exemples de stratégies basées sur l'identité pour AWS la gestion des 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 pour un compte.
`account:GetAlterna teContact`	Lecture	Accorde l'autorisation de récupérer les autres contacts d'un compte.
`account:GetContact Information`	Lecture	Accorde l'autorisation de récupérer les informations de contact principal pour un compte.
`account:GetPrimary Email`	Lecture	Accorde l'autorisation de récupérer l'adresse e-mail principale d'un compte.
`account:GetRegion0 ptStatus`	Lecture	Accorde l'autorisation d'obtenir le statut d'une vérification de l'état de préparation.
`account:AcceptPrim aryEmailUpdate`	Écrire	Accorde l'autorisation d'accepter la mise à jour de l'adresse e-mail principale du

Nom de l'autorisation	Niveau d’accès	Description
		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 autres contacts d'un compte.
`account:DisableRegion`	Écrire	Accorde l'autorisation de désactiver l'utilisation d'une région.
`account:EnableRegion`	Écrire	Accorde l'autorisation d'activer l'utilisation d'une région.
`account:PutAccountName`	Écrire	Accorde l'autorisation de mettre à jour le nom d'un compte.
`account:PutAlternateContact`	Écrire	Accorde l'autorisation de modifier les autres contacts d'un compte.

Nom de l'autorisation	Niveau d’accès	Description
`account:PutContactInformation`	Écrire	Accorde l'autorisation de mettre à jour les informations de contact principal pour 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 identifier et résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Account Management et IAM.

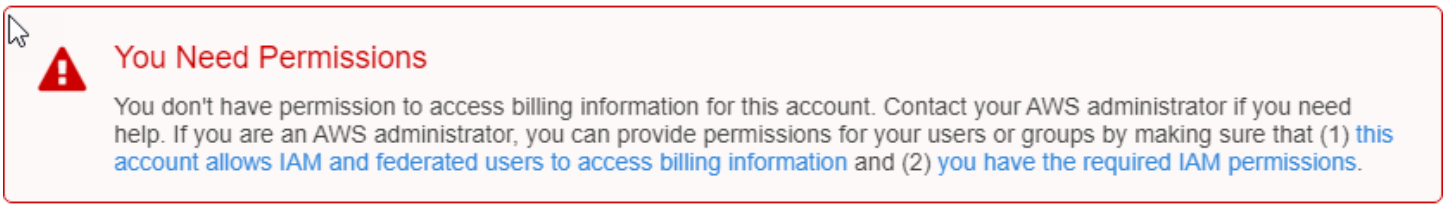
Rubriques

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

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

Si la AWS Management Console indique que vous n'êtes pas autorisé à exécuter 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 tente 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 une erreur selon laquelle vous n'êtes pas autorisé à exécuter l'`iam:PassRole`action, vos stratégies doivent être mises à jour afin de vous permettre de transmettre 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 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 exécuter une action dans Account Management. 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 encore besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je veux autoriser des personnes extérieures à mon 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 stratégies

basées sur les ressources ou les listes de contrôle d'accès (ACLs), vous pouvez utiliser ces stratégies pour accorder aux personnes l'accès à vos ressources.

Pour plus d’informations, consultez les éléments suivants :

- Pour savoir si Account Management prend en charge ces fonctionnalités, consultezComment fonctionne la gestion des AWS comptes avec IAM.
- Pour savoir comment fournir un accès à vos ressources à des Comptes AWS dont vous êtes propriétaire, veuillez consulter Octroi de l'accès à un utilisateur IAM dans un autre 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, veuillez consulter Octroi de l'accès à des Comptes AWS appartenant à 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 en savoir plus sur la différence entre l’utilisation des rôles et des politiques basées sur les ressources pour l’accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l’utilisateur IAM.

AWS politiques gérées pour la gestion des AWS comptes

AWS La gestion des comptes propose actuellement deux politiques AWS gérées que vous pouvez utiliser :

- AWS politique gérée : AWSAccount ManagementReadOnlyAccess
- AWS politique gérée : AWSAccount ManagementFullAccess
- Mises à jour des politiques AWS gérées relatives à la gestion des comptes

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées 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.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. 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 politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle politique Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

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

AWS politique gérée : AWSAccount ManagementReadOnlyAccess

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

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

- Les métadonnées concernant votre Comptes AWS
- Les Régions AWS qui sont activées ou désactivées pour le Compte AWS (vous pouvez consulter le statut des régions dans votre compte uniquement à l'aide de la AWS console)

Pour ce faire, il autorise l'exécution de n'importe laquelle `Get*` des `List*` opérations. Il ne permet pas de modifier les métadonnées du compte ou d'activer ou Régions AWS de désactiver le compte.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `account`— Permet aux principaux de récupérer les informations de métadonnées relatives à Comptes AWS. Cela permet également aux principaux de répertorier Régions AWS les informations activées pour le compte dans le AWS Management Console.

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

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

AWS politique gérée : AWSAccount ManagementFullAccess

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

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

- Les métadonnées concernant votre Comptes AWS
- Les Régions AWS régions activées ou désactivées pour le Compte AWS (vous pouvez consulter le statut ou activer ou désactiver les régions pour votre compte uniquement à l'aide de la AWS console)

Pour ce faire, il autorise l'exécution de toutes `account` les opérations.

Détails de l’autorisation

Cette politique inclut les autorisations suivantes.

- `account`— Permet aux principaux d'afficher ou de modifier les informations de métadonnées relatives à Comptes AWS. Cela permet également aux principaux de répertorier Régions AWS les personnes activées pour le compte et de les activer ou de les désactiver dans le AWS Management Console.

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

Mises à jour des politiques AWS gérées relatives à la gestion des comptes

Consultez les détails des mises à jour apportées aux politiques AWS 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 fil RSS sur la page d'historique des documents de gestion des comptes.

Modification	Description	Date
AWS La gestion des comptes a été lancée avec de nouvelles politiques AWS gérées et a commencé à suivre les modifications	La gestion des comptes a été initialement lancée avec les politiques AWS gérées suivantes : • AWSAccountManagementReadOnlyAccess • AWSAccountManagementFullAccess	30 septembre 2021

Validation de conformité pour la gestion des AWS comptes

Des auditeurs tiers évaluent la sécurité et la conformité des AWS services qui peuvent être exécutés chez vous 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 obtenir la liste des AWS services concernés par des programmes de conformité spécifiques, voir Services AWS champ d'application par programme Services AWS de conformité ou . Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, reportez-vous à la section Téléchargement de rapports dans la section AWS Artifact le Guide de AWS Artifact l'utilisateur.

Lorsque vous utilisez des services, votre Compte AWS responsabilité en matière de conformité dépend de la sensibilité de vos données, des objectifs de conformité de votre entreprise et des lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

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

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité AWS qui vous permet de vérifier votre conformité aux normes et aux meilleures pratiques du secteur de la sécurité.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience dans la gestion des AWS comptes

L'infrastructure AWS mondiale est construite autour Régions AWS de 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 davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

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

Sécurité de l'infrastructure dans Gestion de compte AWS

En tant que services gérés, AWS les services exécutés sur votre Compte AWS site sont protégés par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

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 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.

Surveillez votre Compte AWS

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. AWS fournit 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 appelés AWS, 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 CloudTrail Guide 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.

Enregistrement des appels d'API de gestion de AWS compte à l'aide de AWS CloudTrail

La gestion APIs des AWS comptes est intégrée à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou à un AWS service qui appelle une opération de gestion de compte. CloudTrailcapture tous les appels de l'API de gestion des comptes sous forme d'événements. Les appels capturés incluent tous les appels relatifs aux opérations de gestion des comptes. Si vous créez un suivi, vous pouvez activer la diffusion continue des CloudTrail événements vers un compartiment Amazon S3, y compris les événements relatifs aux opérations de gestion des comptes. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a appelé une opération de gestion de compte, l'adresse IP utilisée pour effectuer la demande, l'auteur de la demande et quand, ainsi que des informations supplémentaires.

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

Informations de gestion de compte dans CloudTrail

CloudTrail est activé dans votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans le cadre d'une opération de gestion de compte, CloudTrail enregistre cette activité dans un CloudTrail événement ainsi que d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements survenus dans votre entreprise Compte AWS, y compris des événements liés aux opérations de gestion de compte, créez un historique. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un parcours dans le AWS Management Console, celui-ci s'applique à tous Régions AWS. Le journal de suivi consigne les événements de toutes les régions dans la partition AWS , et il livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. Vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

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

AWS CloudTrail enregistre toutes les opérations de l'API de gestion des comptes figurant dans la section Référence des API de ce guide. Par exemple, les appels aux `PutAlternateContact` opérations `CreateAccount`, `DeleteAlternateContact`, et génèrent des entrées dans les fichiers CloudTrail journaux.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été faite avec les informations d'identification de l'utilisateur root ou de l'utilisateur AWS Identity and Access Management (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 demande a été faite par un autre AWS service

Pour de plus amples informations, veuillez consulter l'élément userIdentity CloudTrail .

Comprendre les entrées du journal de gestion des comptes

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'opération demandée, la date et l'heure de l'opération, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

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

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 CloudTrail journal pour un appel à l'`PutAlternateContact`opération visant à ajouter un nouveau contact `BILLING` 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 CloudTrail journal pour un appel à l'`DeleteAlternateContact`opération visant à supprimer le contact `OPERATIONS` alternatif actuel.

```
{
  "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'autres Services 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 le `GetRegionOptStatus` et : `ListRegions` APIs

- `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 de la région.

```
{
   "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"
      ]
   }
}
```

Résolvez votre Compte AWS

Utilisez les informations contenues dans les rubriques suivantes pour vous aider à diagnostiquer et à résoudre les problèmes liés à votre Compte 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 AWS connexion.

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 d'autres problèmes liés à Comptes 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	Créez un 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-tentatives infructueuses	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 (adresse) 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'utilisateur AWS 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 de AWS 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 de AWS 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 d'autres problèmes liés à Comptes AWS

Utilisez les informations fournies ici pour vous aider à résoudre les problèmes liés à votre Compte AWS.

Problèmes

- Je dois changer la carte de crédit de mon Compte AWS
- Je dois signaler une Compte AWS activité frauduleuse
- Je dois fermer mon Compte AWS

Je dois changer la carte de crédit de mon Compte AWS

Pour modifier votre carte de crédit Compte AWS, vous devez être en mesure de vous connecter. AWS dispose de protections qui vous obligent à prouver que vous êtes le propriétaire du compte. Pour obtenir des instructions, consultez la section Gestion de vos modes de paiement par carte de crédit dans le guide de AWS Billing l'utilisateur.

Je dois signaler une Compte AWS activité frauduleuse

Si vous soupçonnez une activité frauduleuse utilisant votre compte Compte AWS et que vous souhaitez le signaler, consultez la section Comment signaler un abus de AWS ressources.

Si vous rencontrez des difficultés avec un achat effectué sur Amazon.com, contactez le service client Amazon.

Je dois fermer mon Compte AWS

Pour obtenir de l'aide pour résoudre les problèmes liés à la fermeture de votre Compte AWS, consultezFermez un Compte AWS.

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 après sa 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 l'adresse e-mail que vous avez enregistrée au Compte AWS 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. Pour de plus amples informations, veuillez consulter Mettre à jour l'adresse e-mail de l'utilisateur root (adresse).

- 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 les 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 suivant 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 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.
- Après la fermeture d'un compte, nous AWS enverrons des e-mails quotidiens jusqu'à cinq jours avant de suspendre le domaine. Une fois le domaine suspendu, et selon le bureau

d'enregistrement du domaine, nous supprimerons le domaine dans les 30 jours ou le remettrons à son bureau d'enregistrement. Pour plus d'informations, voir Mon domaine Compte AWS est fermé ou définitivement fermé et mon domaine est enregistré auprès de Route 53.

- AWS CloudTrail est un service de sécurité fondamental. Cela signifie que les sentiers créés par les utilisateurs peuvent continuer à exister et à générer des événements même après leur fermeture, à moins qu'un utilisateur ne supprime explicitement les sentiers qu'ils contiennent Compte AWS avant de les fermer. Compte AWS Pour plus d'informations sur la procédure à suivre pour demander la suppression d'un Compte AWS sentier après la fermeture d'un sentier, consultez Compte AWS la section Fermeture et sentiers 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 SDKs. 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. Cette option n'est disponible que lorsqu'une AWS organisation est en mode Toutes les fonctionnalités.

   > **Note**
   >
   > Si votre organisation utilise le mode de facturation consolidée, le bouton Fermer ne s'affichera pas dans la console. Pour fermer un compte en mode de facturation consolidée, connectez-vous au compte que vous souhaitez fermer en tant qu'utilisateur root. Sur la page Comptes, cliquez sur le bouton Fermer le compte, entrez votre identifiant de compte, puis cliquez sur le bouton Fermer le compte.

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.

> **Note**
>
> Tout compte de membre que vous fermez affichera une `SUSPENDED` étiquette à côté de son nom dans la AWS Organizations console jusqu'à 90 jours après la date de

fermeture initiale. Après 90 jours, le compte du membre ne sera plus affiché dans le AWS Organizations.

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 de membre en utilisant AWS CLI et SDKs

Pour savoir comment fermer un compte membre à l'aide du AWS CLI et SDKs, consultez la section Fermeture d'un compte membre dans votre organisation dans le Guide de AWS Organizations l'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 SDKs. 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 jusqu'à 90 jours après la date de fermeture initiale. Après 90 jours, le compte du membre ne sera plus affiché 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.

La fermeture du compte peut ne pas avoir lieu immédiatement dans toutes les régions et tous les services et peut prendre plusieurs heures.

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 le contenu et les ressources de votre compte (à l'exception des CloudTrail sentiers). 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.

Référence d’API

Les opérations d'API dans l'espace de noms Account Management (`account`) vous permettent de modifier votre Compte AWS.

Chacun Compte AWS prend 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 à l'utilisateur root du compte. 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

Par défaut, les opérations d'API décrites dans ce guide s'appliquent directement au compte qui appelle l'opération. L'identité du compte qui appelle l'opération est généralement un rôle IAM ou un utilisateur IAM et doit être autorisée par une politique IAM pour appeler l'opération d'API. Vous pouvez également appeler ces opérations d'API à partir d'une identité enregistrée dans un compte de AWS Organizations gestion et spécifier le numéro d'identification du compte pour tous Compte AWS les membres de l'organisation.

Version de l'API

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

> **Note**
>
> Au lieu d'utiliser directement l'API, vous pouvez utiliser l'une d'entre elles AWS SDKs, qui comprend des bibliothèques et des exemples de code pour différents langages de programmation et plateformes (Java, Ruby, .NET, iOS, Android, etc.). Ils SDKs fournissent un moyen pratique de créer un accès programmatique aux AWS Organizations. Par exemple, ils s' SDKs occupent de signer les demandes de manière cryptographique, de gérer les erreurs et de réessayer automatiquement les demandes. Pour plus d'informations sur les AWS SDKs, notamment sur la manière de les télécharger et de les installer, consultez la section Outils pour Amazon Web Services.

Nous vous recommandons d'utiliser le AWS SDKs 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, consultez Appel de l'API à l'aide de demandes de requête HTTP le guide de l'utilisateur de Account Management. Organizations prend 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 à AWS, vous devez les signer AWS afin d'identifier leur expéditeur. Vous signez les demandes avec votre clé AWS 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. Une autre option consiste à utiliser le AWS Security Token Service pour générer des informations d'identification de sécurité temporaires et à utiliser ces informations d'identification pour signer les demandes.

Pour signer les 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 qui nécessitent la version 4 indique cette exigence. Pour plus d'informations, consultez la section Signature des demandes AWS d'API dans le guide de l'utilisateur IAM.

Lorsque vous utilisez l'interface de ligne de AWS commande (AWS CLI) ou l'une des interfaces AWS SDKs pour envoyer des demandes AWS, ces outils signent automatiquement les demandes à votre place avec la clé d'accès que vous spécifiez lors de la configuration des outils.

Support et commentaires pour la gestion des comptes

Nous apprécions vos commentaires. Envoyez vos commentaires à feedback-awsaccounts@amazon.com ou publiez vos commentaires et questions sur le forum d'assistance à la gestion des comptes. Pour plus d'informations sur les forums AWS d'assistance, consultez l'aide des forums.

Comment les exemples sont présentés

Le 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 pour améliorer la lisibilité. Lorsque les exemples de paramètres d'entrée se traduisent également par de longues chaînes qui s'étendent au-delà de l'écran, nous insérons des sauts de ligne pour améliorer la lisibilité. Vous devez toujours soumettre l'entrée sous forme de chaîne de texte JSON unique.

Enregistrement des demandes d'API

Account Management prend CloudTrail en charge un service qui enregistre les appels d' AWS API pour vous Compte AWS et fournit des fichiers journaux à un compartiment Amazon S3. En utilisant les informations collectées par CloudTrail, vous pouvez déterminer quelles demandes ont été adressées avec succès à la gestion du compte, qui a fait la demande, quand elle a été faite, etc. Pour en savoir plus sur la gestion des comptes et sa prise en charge CloudTrail, consultezEnregistrement des appels d'API de gestion de AWS compte à l'aide de AWS CloudTrail. Pour en savoir plus CloudTrail, notamment comment l'activer et trouver vos fichiers journaux, consultez le guide de l'AWS CloudTrail utilisateur.

Actions

Les actions suivantes sont prises en charge :

- AcceptPrimaryEmailUpdate
- DeleteAlternateContact
- DisableRegion
- EnableRegion
- GetAccountInformation
- GetAlternateContact
- GetContactInformation
- GetPrimaryEmail
- GetRegionOptStatus
- ListRegions
- PutAccountName
- 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 : String

Modèle : `\d{12}`

Obligatoire : oui

Otp

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

Type : String

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 : String

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 : String

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. 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

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 langages spécifiques AWS SDKs, consultez ce qui suit :

- 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 Kotlin
- 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 Mettre à jour les contacts secondaires pour votre Compte AWS.

> **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, voir Activer 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 d'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 : String

Modèle : `\d{12}`

Obligatoire : non

AlternateContactType

Spécifie les contacts alternatifs à supprimer.

Type : String

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

{
   "AccountName":"MyAccount"
}
```

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 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.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 langages spécifiques AWS SDKs, consultez ce qui suit :

- 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 Kotlin
- 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 : String

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 : String

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 langages spécifiques AWS SDKs, consultez ce qui suit :

- 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 Kotlin
- 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 : String

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 : String

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 langages spécifiques AWS SDKs, consultez ce qui suit :

- 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 Kotlin

- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

GetAccountInformation

Récupère des informations sur le compte spécifié, notamment son nom de compte, son identifiant de compte, ainsi que la date et l'heure de création du compte. Pour utiliser cette API, un utilisateur ou un rôle IAM doit disposer de l'autorisation `account:GetAccountInformation` IAM.

Syntaxe de la demande

```
POST /getAccountInformation 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 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 d'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 : String

Modèle : `\d{12}`

Obligatoire : non

Syntaxe de la réponse

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

{
   "AccountCreatedDate": "string",
   "AccountId": "string",
   "AccountName": "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.

AccountCreatedDate

Date et heure de création du compte.

Type : Timestamp

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 : String

Modèle : `\d{12}`

AccountName

Le nom du compte.

Type : String

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

Modèle : `[ -;=?-~]+`

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 récupère les informations de compte 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.GetAccountInformation

{}
```

Exemple de réponse

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

{
   "AccountId": "123456789012",
   "AccountName": "MyAccount",
   "AccountCreatedDate": "2020-11-30T17:44:37Z"
}
```

Exemple 2

L'exemple suivant extrait les informations de compte 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.GetAccountInformation

{
   "AccountId": "123456789012"
}
```

Exemple de réponse

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

{
   "AccountId": "123456789012",
   "AccountName": "MyMemberAccount",
   "AccountCreatedDate": "2020-11-30T17:44:37Z"
}
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- 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 Kotlin
- 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 Mettre à jour les contacts secondaires pour votre Compte AWS.

> **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, voir Activer 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 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 d'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 : String

Modèle : `\d{12}`

Obligatoire : non

AlternateContactType

Spécifie le contact alternatif que vous souhaitez récupérer.

Type : String

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 langages spécifiques AWS SDKs, consultez ce qui suit :

- 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 Kotlin
- 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 le contact principal pour votre Compte AWS.

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 : String

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 langages spécifiques AWS SDKs, consultez ce qui suit :

- 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 Kotlin
- 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 d'administrateur délégué d'une organisation pour un compte membre.

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

Type : String

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 : String

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 langages spécifiques AWS SDKs, consultez ce qui suit :

- 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 Kotlin
- 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 : String

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 : String

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 : String

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 : String

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 langages spécifiques AWS SDKs, consultez ce qui suit :

- 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 Kotlin
- 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 : String

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 : String

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 : String

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 langages spécifiques AWS SDKs, consultez ce qui suit :

- 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 Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

PutAccountName

Met à jour le nom du compte spécifié. Pour utiliser cette API, les principaux IAM doivent disposer de l'autorisation `account:PutAccountName` IAM.

Syntaxe de la demande

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

{
   "AccountId": "string",
   "AccountName": "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 d'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 : String

Modèle : `\d{12}`

Obligatoire : non

AccountName

Le nom du compte.

Type : String

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

Modèle : `[ -;=?-~]+`

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 met à jour le nom du compte dont les informations d'identification sont utilisées pour appeler l'opération.

Exemple de demande

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

{
   "AccountName":"MyAccount"
}
```

Exemple de réponse

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

Exemple 2

L'exemple suivant met à jour le nom du 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.PutAccountName

{
   "AccountId": "123456789012",
   "AccountName": "MyMemberAccount"
}
```

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 langages spécifiques AWS SDKs, consultez ce qui suit :

- 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 Kotlin
- 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 Mettre à jour les contacts secondaires pour votre Compte AWS.

> **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, voir Activer 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 d'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 : String

Modèle : `\d{12}`

Obligatoire : non

AlternateContactType

Spécifie le contact alternatif que vous souhaitez créer ou mettre à jour.

Type : String

Valeurs valides : `BILLING | OPERATIONS | SECURITY`

Obligatoire : oui

EmailAddress

Spécifie l'adresse e-mail de l'autre contact.

Type : String

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 : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 64.

Obligatoire : oui

PhoneNumber

Spécifie le numéro de téléphone de l'autre contact.

Type : String

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 : String

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 langages spécifiques AWS SDKs, consultez ce qui suit :

- 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 Kotlin
- 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 le contact principal pour votre Compte AWS.

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 d'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 : String

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 langages spécifiques AWS SDKs, consultez ce qui suit :

- 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 Kotlin
- 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 : String

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 : String

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 : String

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 langages spécifiques AWS SDKs, consultez ce qui suit :

- 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 Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

Actions connexes dans d'autres AWS services

Les opérations suivantes sont liées à l'espace de AWS Organizations noms Gestion de compte AWS mais en font partie :

- CreateAccount
- CreateGovCloudAccount
- DescribeAccount

CreateAccount

L'opération d'`CreateAccount`API ne peut être utilisée que dans le contexte d'une organisation gérée par le AWS Organizations service. L'opération d'API est définie dans l'espace de noms de ce service.

Pour plus d’informations, consultez CreateAccount dans la Référence d’API AWS Organizations .

CreateGovCloudAccount

L'opération d'`CreateGovCloudAccount`API ne peut être utilisée que dans le contexte d'une organisation gérée par le AWS Organizations service. L'opération d'API est définie dans l'espace de noms de ce service.

Pour plus d'informations, consultez CreateGovCloudAccount dans la Référence d'API AWS Organizations .

DescribeAccount

L'opération d'`DescribeAccount`API ne peut être utilisée que dans le contexte d'une organisation gérée par le AWS Organizations service. L'opération d'API est définie dans l'espace de noms de ce service.

Pour plus d'informations, consultez DescribeAccount dans la Référence d'API AWS Organizations .

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 : String

Valeurs valides : `BILLING | OPERATIONS | SECURITY`

Obligatoire : non

EmailAddress

Adresse e-mail associée à cet autre contact.

Type : String

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 : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 64.

Obligatoire : non

PhoneNumber

Le numéro de téléphone associé à cet autre contact.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 25

Modèle : `[\s0-9()+-]+`

Obligatoire : non

Title

Titre associé à ce contact alternatif.

Type : String

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 langages spécifiques AWS SDKs, consultez ce qui suit :

- 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 : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 60.

Obligatoire : oui

City

Ville de l'adresse de contact principale.

Type : String

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 : String

Contraintes de longueur : longueur fixe de 2.

Obligatoire : oui

FullName

Nom complet de l'adresse de contact principale.

Type : String

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 : String

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 : String

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 : String

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 : String

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 : String

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 : String

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 d'Amérique, 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 : String

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 : String

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 langages spécifiques AWS SDKs, consultez ce qui suit :

- 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 : String

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 : String

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 langages spécifiques AWS SDKs, consultez ce qui suit :

- 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 : String

Obligatoire : oui

name

Nom du champ dans lequel l'entrée non valide a été détectée.

Type : String

Obligatoire : oui

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- 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 la version 4 de Signature, consultez la section Signing AWS API du guide de l'utilisateur IAM.

Action

Action à effectuer.

Type : chaîne

Obligatoire : oui

Version

Version de l'API pour laquelle la demande est écrite, exprimée dans le format YYYY-MM-DD.

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' AWS API 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 et l'heure suivantes sont une X-Amz-Date valeur valide :`20120325T120000Z`.

Condition : X-Amz-Date est un en-tête facultatif pour toutes les demandes. Il peut être utilisé pour signer les demandes. Si l'en-tête Date est spécifié au format de base ISO 8601, X-Amz-Date il n'est pas obligatoire. Lorsqu'il 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' AWS API dans le Guide de l'utilisateur IAM.

Type : chaîne

Obligatoire : Conditionnelle

X-Amz-Security-Token

Le jeton de sécurité temporaire obtenu par un appel à AWS Security Token Service (AWS STS). Pour obtenir la liste des services prenant en charge les informations d'identification de sécurité temporaires d' AWS STS, consultez Services AWS qui fonctionnent avec IAM dans le Guide de l'utilisateur IAM.

Condition : Si vous utilisez des informations d'identification de sécurité temporaires provenant de AWS 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 Créer une demande d' AWS API 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 AWS services. 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 demande n'est pas conforme aux AWS normes.

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 AWS l'ID de clé d'accès fourni 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' AWS accès nécessite un abonnement au service.

Code d'état HTTP : 403

RequestExpired

La demande est parvenue au service plus de 15 minutes après l'horodatage sur la demande ou plus de 15 minutes après la date d'expiration de la demande (par exemple pour les demandes pré-signées URLs), ou le horodatage sur la demande est daté dans plus de 15 minutes dans le futur.

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 AWS service.

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 de requête pour la gestion des AWS comptes. Pour plus d'informations sur le fonctionnement de l'API et les erreurs, consultez le Référence d'API.

> **Note**
>
> Au lieu de passer des appels directs à l'API AWS Account Management Query, vous pouvez utiliser l'un des AWS SDKs. Il AWS SDKs s'agit de bibliothèques et d'exemples de code pour différents langages de programmation et plateformes (Java, Ruby, .NET, iOS, Android, etc.).

Ils SDKs fournissent un moyen pratique de créer un accès programmatique à la gestion des AWS comptes et AWS. Par exemple, ils se SDKs chargent de tâches telles que la signature cryptographique des demandes, la gestion des erreurs et le renouvellement automatique des demandes. Pour plus d'informations AWS SDKs, notamment sur la manière de les télécharger et de les installer, consultez la section Outils pour Amazon Web Services.

Avec l'API de requête pour la gestion des AWS comptes, vous pouvez appeler des actions de service. Les requêtes de l'API de requête sont des requêtes HTTPS qui doivent contenir un `Action` paramètre pour indiquer l'opération à effectuer. AWS La gestion des comptes prend en charge `GET` et `POST` demande toutes les opérations. En d'autres termes, l'API ne vous oblige pas à l'utiliser `GET` pour certaines actions et `POST` pour d'autres. Toutefois, les `GET` demandes sont soumises à la limite de taille d'une URL. Bien que cette limite dépend du navigateur, elle est généralement de 2 048 octets. Par conséquent, pour les demandes d'API de requête qui nécessitent des tailles plus importantes, vous devez utiliser une `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 d'API.

Rubriques

- Points de terminaison
- HTTPS requis
- Signature des demandes de l'API de gestion des AWS comptes

Points de terminaison

AWS Account Management dispose d'un point de terminaison API mondial unique hébergé dans l'est des États-Unis (Virginie du Nord) Région AWS.

Pour plus d'informations sur les AWS points de terminaison et les régions pour tous les services, voir 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 les informations d'identification de sécurité, vous devez utiliser le protocole HTTPS pour chiffrer toutes les demandes d'API.

Signature des demandes de l'API de gestion des AWS comptes

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 les informations d'identification de votre compte AWS root dans le cadre de vos tâches quotidiennes liées à la gestion des AWS comptes. Vous pouvez utiliser les informations d'identification d'un utilisateur AWS Identity and Access Management (IAM) ou des 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 section Signing AWS API du guide de l'utilisateur IAM.

Pour plus d’informations, consultez les ressources suivantes :

- Informations d'identification de sécuritéAWS : fournit des informations générales sur les types d'informations d'identification que vous pouvez utiliser pour accéder à AWS.
- Bonnes pratiques de sécurité dans le domaine de l'IAM : propose des suggestions d'utilisation du service IAM afin de sécuriser vos AWS ressources, y compris celles relatives à la gestion des AWS comptes.
- Informations d'identification de sécurité temporaires dans IAM : décrit comment créer et utiliser des informations d'identification de sécurité temporaires.

Quotas pour Gestion de compte AWS

Vous Compte AWS disposez de quotas par défaut, anciennement appelés limites, pour chaque AWS service. 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 maximum de `StartPrimaryEmailUpdate` demandes par compte cible	3 par 30 secondes
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	50
Taux de `AcceptPrimaryEmailUpdate` demandes par compte appelant	1 par seconde, rafale à 1 par seconde
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 `GetAccountInformation` demandes par compte appelant	3 par seconde, rafale à 3 par seconde
Taux de `GetAlternateContact` demandes par compte	10 par seconde, rafale à 15 par seconde

Ressource	Quota
Taux de `GetContactInformation` demandes par compte	10 par seconde, rafale à 15 par seconde
Taux de `GetPrimaryEmail` demandes par compte appelant	3 par seconde, rafale à 3 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
Taux de `PutAccountName` demandes par compte appelant	1 par seconde, rafale à 1 par seconde
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
Taux de `StartPrimaryEmailUpdate` demandes par compte appelant	1 par seconde, rafale à 1 par seconde

Gérer des comptes en Inde

Si vous en souscrivez un nouveau Compte AWS et que vous choisissez l'Inde comme adresse de contact et de facturation, votre contrat d'utilisation est conclu avec Amazon Web Services India Private Limited (AWS Inde), un vendeur AWS local en Inde. AWS L'Inde gère votre facturation, et le total de votre facture est indiqué en roupies indiennes (INR) au lieu de dollars américains (USD). Pour plus d'informations sur la gestion d'un Compte AWS, consultezConfigurez votre Compte AWS.

Si votre compte est en AWS Inde, suivez les procédures décrites dans cette rubrique pour gérer votre compte. Cette rubrique explique comment créer un compte AWS en Inde, modifier les informations relatives à AWS votre compte en Inde, gérer la vérification des clients et ajouter ou modifier votre numéro de compte permanent (PAN).

Dans le cadre de la vérification de la carte de crédit lors de l'inscription, AWS l'Inde débite votre carte de crédit de 2 INR. AWS L'Inde rembourse les 2 INR après vérification. Dans le cadre du processus de vérification, vous pouvez être redirigé vers votre banque.

Rubriques

Créez un accord Compte AWS avec AWS l'Inde

AWS L'Inde est un vendeur local AWS de produits en Inde. Si votre adresse de contact et de facturation se trouvent en Inde et que vous souhaitez créer un compte, suivez la procédure ci-dessous pour créer AWS un compte en Inde.

Pour ouvrir un compte AWS en Inde

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. Si Créer un nouveau compte

n'est Compte AWS toujours pas visible, choisissez Se connecter à un autre compte, puis choisissez Créer un nouveau compte Compte AWS.

3. Entrez les informations de votre compte, vérifiez votre adresse e-mail et choisissez un mot de passe fort pour votre compte.
4. Choisissez Professionnel ou Personnel. Les comptes personnels et les comptes professionnels présentent les mêmes caractéristiques et fonctions.
5. Entrez les coordonnées de votre entreprise ou personnelles. Si votre adresse de contact ou de facturation est basée en Inde, conformément aux réglementations de l'équipe indienne d'intervention en cas d'urgence informatique (Cert-in) AWS , elle est tenue de collecter et de valider vos informations d'identité avant de vous accorder l'accès AWS aux services.

   Le nom que vous avez choisi entre vos coordonnées ou vos informations de facturation doit correspondre exactement au nom qui apparaît sur le document que vous prévoyez d'utiliser pour la vérification des clients. Par exemple, si vous envisagez de vérifier un compte professionnel à l'aide d'un certificat de constitution, vous devez fournir le nom de l'entreprise qui apparaît sur le document. Pour obtenir la liste des types de documents acceptés, consultez the section called “Documents indiens acceptés pour la vérification du client”.
6. Après avoir lu le contrat client, cochez la case Termes et conditions, puis choisissez Continuer.
7. Sur la page Informations de facturation, saisissez le mode de paiement que vous souhaitez utiliser. Vous devez fournir votre valeur CVV dans le cadre du processus de vérification.
8. Sous Avez-vous un PAN ? , choisissez Oui si vous avez un numéro de compte permanent (PAN) que vous souhaitez voir apparaître sur vos factures fiscales, puis saisissez votre PAN. Si vous n'avez pas de PAN ou si vous souhaitez l'ajouter après votre inscription, choisissez Non.
9. Choisissez Verify et continuez. AWS L'Inde débite votre carte de 2 INR dans le cadre du processus de vérification. AWS L'Inde rembourse les 2 INR après vérification.
10. Sur la page Confirmer votre identité, sélectionnez l'objectif principal de l'enregistrement du compte.
11. Choisissez le type de propriétaire qui représente le mieux le propriétaire du compte. Si vous choisissez une entreprise, une organisation ou un partenariat comme type de propriété, entrez le nom d'un responsable clé. Le principal responsable peut être un directeur, un chef des opérations ou une personne chargée des opérations de votre entreprise.
12. Selon le type de propriété que vous avez choisi, choisissez un type de document accepté en Inde à utiliser pour la vérification et saisissez les informations de votre document.

> **Note**
>
> Si vous avez un compte personnel et que vous envisagez d'utiliser un permis de conduire qui n'est pas délivré par l'Union de l'Inde, nous vous recommandons d'utiliser un autre type de document personnel à des fins de vérification.

13. Choisissez le nom que vous souhaitez utiliser pour la vérification des clients.

    Les noms figurant dans vos informations de facturation et de contact apparaîtront pour être sélectionnés s'ils sont associés à une adresse indienne. Assurez-vous que le nom que vous choisissez correspond au nom du type de document que vous prévoyez d'utiliser pour la vérification client. Si vous devez modifier le nom associé à votre adresse de facturation ou de contact, vous pouvez le faire après avoir créé votre compte.
14. Donnez votre accord pour soumettre les informations à des fins de vérification, puis choisissez Continuer.

    Vous serez informé du résultat de la vérification client par e-mail une fois que vous aurez terminé la création de votre compte. Vous pouvez également vérifier le statut sur la page de vérification du client dans les paramètres de votre compte ou dans le AWS Health Dashboard ultérieurement. Vous devez passer la vérification client pour accéder aux AWS services.
15. Choisissez si vous souhaitez vérifier votre numéro de téléphone portable par SMS ou par appel vocal.
16. Sélectionnez le code de votre pays ou de votre région, puis entrez votre numéro de téléphone portable.
17. Réalisez le contrôle de sécurité.
18. Choisissez Envoyer un SMS ou Appelez-moi maintenant. Après quelques instants, vous recevrez un code PIN à quatre chiffres dans un SMS ou un appel automatique sur votre téléphone portable.
19. Sur la page Confirmer votre identité, entrez le code PIN que vous avez reçu et choisissez Continuer.
20. Sur la page Sélectionnez un plan d'assistance, sélectionnez votre plan d'assistance, puis choisissez Terminer l'inscription. Une fois votre mode de paiement et votre vérification client vérifiés, votre compte sera activé et vous recevrez un e-mail confirmant l'activation de votre compte.

> **Note**
>
> Si vous avez terminé la vérification client et que vous modifiez le nom, l'adresse ou le document précédemment utilisé pour vérifier votre identité, vous devrez peut-être mettre à jour et terminer à nouveau votre vérification client. Pour de plus amples informations, veuillez consulter the section called “Modifiez les informations de vérification de votre client”.

Gérez les informations de vérification de vos clients

Conformément aux réglementations de l'équipe indienne d'intervention en cas d'urgence informatique (Cert-in), elle AWS est tenue de collecter et de valider vos informations d'identité avant de vous accorder un nouvel accès ou un accès continu aux AWS services. Votre identité doit être vérifiée à l'aide du nom figurant sur l'adresse de facturation ou de contact que vous avez fournie en Inde. Au cours de la vérification, AWS vérifiera si le numéro du document est valide et si le nom que vous fournissez correspond au nom associé au document que vous utilisez pour la vérification auprès du client. Le nom que vous choisissez entre vos coordonnées ou vos informations de facturation doit correspondre exactement au nom qui apparaît sur le document.

Pour mettre à jour votre nom et votre adresse de facturation, consultez la page des préférences de paiement. Pour mettre à jour le nom et l'adresse de votre contact, consultez the section called “Mettez à jour le contact principal de votre Compte AWS”. Si vous modifiez des informations que vous avez précédemment utilisées pour la vérification des clients, telles que le nom ou l'adresse en Inde figurant dans vos informations de facturation ou de contact, vous devrez peut-être mettre à jour et soumettre à nouveau vos informations de vérification client.

Vérifiez le statut de vérification de votre client

Vous pouvez consulter le statut de vérification de votre client à tout moment sur la page de vérification du client. Si votre statut de vérification est Vérification requise ou Échec de la vérification, créez ou mettez à jour les informations de vérification de votre client et soumettez-les pour vérification.

Créez les informations de vérification de votre client

Pour terminer la vérification du client, vous devrez fournir des informations provenant d'un document accepté en Inde. Pour obtenir la liste des types de documents acceptés, consultez the section called “Documents indiens acceptés pour la vérification du client”.

1. Connectez-vous au AWS Management Console.
2. Dans la barre de navigation, dans le coin supérieur droit, choisissez le nom de votre compte (ou alias), puis sélectionnez Compte.
3. Sous Autres paramètres, sélectionnez Vérification du client.

   Si vous n'avez pas encore fourni vos informations de vérification client, vous verrez la page Créer une vérification client.
4. Choisissez le nom qui correspond exactement au nom figurant sur le document que vous prévoyez d'utiliser pour la vérification client. Par exemple, si vous envisagez de vérifier un compte professionnel à l'aide d'un certificat de constitution, vous devez fournir le nom de l'entreprise qui apparaît sur le document.
5. Fournissez les autres informations demandées sur la page. Selon le type de document que vous avez choisi, vous devrez peut-être télécharger une copie du recto et du verso du document. Si vous téléchargez un fichier image, assurez-vous que toutes les informations contenues dans le document sont visibles et lisibles.
6. Sélectionnez Envoyer.

   Vous serez informé du résultat de la vérification client et des prochaines étapes par e-mail ou sur le AWS Health Dashboard.

Modifiez les informations de vérification de votre client

Vous pouvez modifier les informations de vérification de vos clients, telles que l'objectif principal de l'enregistrement du compte, le type de votre organisation, le nom, le type de document, le téléchargement du document ou les informations du document que vous souhaitez utiliser pour la vérification.

Si vous modifiez le nom ou le type de document à utiliser pour la vérification client, ou si vous mettez à jour les informations d'un document, l'enregistrement des modifications nécessitera une nouvelle vérification de votre identité.

1. Connectez-vous au AWS Management Console.
2. Dans la barre de navigation, dans le coin supérieur droit, choisissez le nom de votre compte (ou alias), puis sélectionnez Compte.
3. Sous Autres paramètres, sélectionnez Vérification du client.
4. Choisissez Modifier, puis mettez à jour les informations que vous souhaitez modifier.

   Lorsque vous mettez à jour les informations, tenez compte des instructions suivantes :

   - Si vous choisissez un autre nom, celui-ci doit correspondre exactement au nom figurant sur le document que vous comptez utiliser pour la vérification auprès des clients. Par exemple, si vous envisagez de vérifier un compte professionnel à l'aide d'un certificat de constitution, vous devez fournir le nom de l'entreprise qui apparaît sur le document.
   - Si vous choisissez un autre type de document, vous devrez télécharger une copie du recto et du verso (le cas échéant) du document. Toutes les informations contenues dans le téléchargement du document doivent être visibles et lisibles.
   - Si vous avez un compte personnel et que vous envisagez d'utiliser un permis de conduire qui n'est pas délivré par l'Union de l'Inde, nous vous recommandons d'utiliser un autre type de document personnel à des fins de vérification.

     Pour obtenir la liste des types de documents acceptés, consultez the section called “Documents indiens acceptés pour la vérification du client”.
5. Sélectionnez Envoyer.

   Si votre identité doit être vérifiée à nouveau en raison du type de modifications que vous avez enregistrées, vous serez informé du résultat de la vérification client et des prochaines étapes par e-mail. Vous pouvez également consulter les résultats en retournant sur la page de vérification du client ou dans le AWS Health Dashboard.

Documents indiens acceptés pour la vérification du client

Les types de documents suivants émis par le gouvernement indien sont acceptés pour vérification du client.

> **Note**
>
> Les liens ci-dessous sont susceptibles d'être modifiés par le gouvernement.

- Carte PAN - Disponible en formats numérique et physique, la carte de numéro de compte permanent (PAN) contient un identifiant alphanumérique unique délivré par le département de l'impôt sur le revenu de l'Inde aux particuliers, aux entreprises et aux entités. Un PAN se compose de dix caractères, y compris des lettres et des chiffres, au format **`AAAAA1111A`**. Pour utiliser ce document à des fins de vérification, vous devez également fournir la date de naissance (individuelle) ou la date de constitution (entreprise) qui apparaît sur le document PAN et télécharger le recto de la carte. Vous pouvez vous rendre sur le site officiel du département de l'impôt sur le revenu pour vérifier la validité de votre PAN.
- Carte d'identité d'électeur/EPIC - La carte d'identité d'électeur, également connue sous le nom de carte d'identité avec photo d'électeur (EPIC), contient un numéro d'identification unique délivré par la Commission électorale de l'Inde aux électeurs éligibles en Inde. Un numéro d'identification/EPIC d'électeur est composé de dix caractères, y compris des lettres et des chiffres. Vous pouvez vous rendre sur le site officiel de la Commission électorale de l'Inde pour vérifier la validité de votre carte d'électeur. Pour utiliser ce document à des fins de vérification, vous devez télécharger le recto et le verso de la carte.
- Permis de conduire - Si votre permis de conduire n'est pas délivré par l'Union indienne, nous vous recommandons d'utiliser un autre type de document à des fins de vérification. Un numéro de permis de conduire est composé de 12 à 16 caractères, dont des lettres, des chiffres, un espace ou un trait d'union. Pour utiliser ce document à des fins de vérification, vous devez fournir votre date de naissance et télécharger le recto et le verso de la carte. Vous pouvez vous rendre sur le site Parivahan Sewa du ministère des Transports routiers et des Autoroutes pour vérifier la validité de votre permis de conduire.
- Passeport - Le passeport sert de preuve de citoyenneté indienne et peut être utilisé comme pièce d'identité pour les voyages internationaux. Dans les passeports délivrés par le Passport Seva Kendra (PSK), le numéro de dossier de passeport est un identifiant alphanumérique unique associé au passeport d'un individu. Un numéro de dossier de passeport est composé de quinze caractères, y compris des lettres et des chiffres. Différent du numéro de passeport, le numéro de dossier de passeport se trouve sur l'une des dernières pages de votre passeport indien. Pour utiliser ce document à des fins de vérification, vous devez fournir votre date de naissance et télécharger la première page et la dernière page (contenant le numéro de dossier du passeport) du passeport. Vous pouvez vous rendre sur le site Passport Seva Kendra du ministère des Affaires extérieures pour vérifier la validité de votre numéro de dossier de passeport.

> **Note**
>
> Pour la vérification par le client, seul le numéro de dossier de passeport d'un passeport indien délivré en Inde est accepté. Si votre passeport indien a été délivré dans un autre pays, vous devez utiliser un autre document indien pour la vérification auprès du client.

- Certificat de constitution - Un certificat de constitution est un document délivré par le ministère des Affaires commerciales (MCA) qui date de l'enregistrement d'une entreprise en tant qu'entité juridique. Le certificat est utilisé pour identifier et suivre de manière unique les entreprises enregistrées en Inde. Chaque certificat contient un numéro d'identification d'entreprise (CIN), qui est un identifiant alphanumérique unique composé de 21 caractères, y compris des lettres et des chiffres. Pour utiliser ce document à des fins de vérification, vous devez télécharger le certificat de constitution. Vous pouvez vous rendre sur le portail du ministère des Affaires commerciales pour vérifier la validité de votre CIN.

Différents types de documents indiens sont acceptés pour les comptes personnels et professionnels :

- Pour les comptes personnels : carte PAN, carte d'électeur (EPIC), permis de conduire et passeport.
- Pour les comptes professionnels - carte PAN et certificat de constitution.

Gérez votre AWS compte en Inde

À l'exception des tâches suivantes, les procédures de gestion de votre compte sont les mêmes que celles des comptes créés en dehors de l'Inde. Pour obtenir des informations générales sur la gestion de votre compte, consultezConfigurez votre compte.

Utilisez le AWS Management Console pour effectuer les tâches suivantes :

- Ajouter ou modifier un numéro de compte permanent
- Modification de plusieurs numéros de compte permanents
- the section called “Gérez les informations de vérification de vos clients”
- Modifier plusieurs numéros de taxe sur les produits et services (GSTs)
- Afficher une facture fiscale

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
Nouveau nom de compte APIs	Support pour créer un nouveau `GetAccountInformation` compte et `PutAccountName` APIs pour consulter ou modifier un nom de compte.	22 avril 2025
Fin du support pour la modification des questions relatives aux défis de sécurité	La rubrique Modifier vos questions relatives aux défis de sécurité a été supprimée du guide car le support est terminé.	6 janvier 2025
Nouvel e-mail principal APIs	Support pour les nouvelles `GetPrimaryEmail` adresses e-mail de l'utilisateur root et `AcceptPrimaryEmailUpdate` APIs pour la mise à jour centralisée de l' pour tout compte membre dans AWS Organizations. `StartPrimaryEmailUpdate` Pour plus d'informations, consultez la section Mise à jour de l'adresse e-mail de l'utilisateur root () pour un compte 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.	1er 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 nouvelles questions de défi a été supprimée de la page des comptes.	5 janvier 2024
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 informations de contact APIs	Support pour les nouveaux `GetContactInformation` et `PutContactInformation` APIs.	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	Première publication du guide de référence AWS sur la gestion des comptes	30 septembre 2021

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.