Guide de l’utilisateur

AWS Gestion du compte

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

AWS Gestion du compte: Guide de l’utilisateur

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

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

Table of Contents

Qu'est-ce qu'un Compte AWS? 1
Caractéristiques d'un Compte AWS 3
C'est la première fois AWS utilisateur ? 3
Support et commentaires 4
Autre AWS resources 4
Comparez les options d'inscription 6
Pris en charge Services AWS pour Inscrivez-vous pour AWS (nouveau) 6
Services AWS inclus dans le niveau gratuit de notre nouveau AWS expérience 7
Services AWS inclus dans le plan payant de notre nouveau AWS expérience 12
Services AWS non pris en charge pour notre nouveau AWS expérience 13
Considérations relatives au choix du mode d'inscription à AWS 18
Comparez les fonctionnalités des options d'inscription 18
Comparaison de la gestion des accès 20
Gérez votre Comptes AWS 22
Inscrivez-vous pour AWS (nouveau) 26
Inscrivez-vous en utilisant S'inscrire pour AWS (nouveau) 28
Étapes suivantes 29
AWS Paramètres d'utilisation 30
Connectez un outil de codage basé sur l'IA 31
Considérations relatives à la connexion de votre outil de codage à votre projet 31
Connectez votre outil de codage IA à votre projet 32
Travaillez sur plusieurs projets 33
AWS actions pour les porteurs de projets 35
Mettez à jour votre mot de passe 36
Gérer l'authentification multifactorielle (MFA) 37
Points clés 38
Types de MFA disponibles pour notre nouveau AWS expérience 38
Enregistrez votre appareil MFA 40
Enregistrez une clé de sécurité en tant que dispositif MFA 42
Renommez votre appareil MFA 42
Supprimer votre appareil MFA 43
Supprimer toutes les sessions 43
Gérez votre nom ou votre surnom 44
Changez votre adresse e-mail 45

Modifier vos informations de contact 46
Refuser l'utilisation de votre contenu à des fins d'amélioration du service 46
Demandez vos données AWS Builder ID 47
Création d'un projet 48
Considérations relatives à la création d'un projet 49
Pour créer un projet 49
Régions AWS pour vos projets 50
Trouvez la sélection Région AWS pour vos projets 51
Pays où des ressources régionales sont approvisionnées dans l'est des États-Unis (Ohio) (us-east-2) 52
Pays où des ressources régionales sont fournies en Asie-Pacifique (Sydney) (ap-southeast-2) 54
Pays où des ressources régionales sont fournies en Europe (Stockholm) (eu-north-1) 58
Politiques gérées pour votre organisation 64
Politiques de contrôle des services pour les projets 65
Politiques de contrôle des services pour le niveau gratuit pour les projets 86
Politiques de contrôle des services pour le plan payant pour les projets 97
Politiques de contrôle des ressources pour les projets 109
Basculer entre les projets 111
Passez d'un projet à l'autre pour les sessions actives à partir du Console de gestion AWS .. 111
Passez d'un projet à l'autre dans AWS Settings 112
Passez d'un projet à l'autre depuis Console de gestion AWS 112
Inviter des membres de l'équipe 112
Considérations pour les membres de l'équipe 113
Comment les membres de l'équipe accèdent à votre AWS resources 114
Inviter des membres de l'équipe 115
Inviter un membre de l'équipe à participer à un projet 115
Supprimer un membre de l'équipe d'un projet 116
Supprimer un membre de l'équipe 117
Révoquer une invitation 117
Renvoyer une invitation 118
Améliorez votre compte 119
Considérations relatives à la mise à niveau de votre compte 119
Améliorez votre compte 120
Créer une limite de dépenses 120
Qu'est-ce qu'une limite de dépenses ? 120

Définissez votre limite de dépenses 121
Notifications 122
Personnalisez vos paramètres de limite de dépenses grâce à des contrôles anticipés des coûts optionnels 122
Que se passe-t-il si vous atteignez votre limite 123
Autres points importants à noter 124
Créez une limite de dépenses dans AWS Settings 124
Mettre à jour une limite de dépenses 125
Mettre à jour une limite de dépenses dans AWS Settings 125
Supprimer une limite de dépenses 126
Supprimer une limite de dépenses dans AWS Settings 126
Offre gratuite 126
Suivi de votre utilisation de l'offre gratuite 127
Gagnez des crédits supplémentaires 129
Consultez vos informations de facturation dans AWS Settings 129
Pour consulter vos coûts par projet 130
Consultez votre historique de facturation dans AWS Settings 130
Gérez votre mode de paiement 131
Effectuez un paiement en AWS Settings 132
Changez votre devise préférée en AWS Settings 133
Gérez l'enregistrement fiscal dans AWS Settings 133
Mise à jour et suppression de numéros d'enregistrement fiscal 134
Gestion de vos exonérations fiscales américaines 134
Afficher et échanger des crédits 135
Gérer des comptes en Inde 136
Inscrivez-vous pour AWS (nouveau) avec AWS Inde 137
Gérez les informations de vérification de vos clients 139
Configurez votre facturation en Inde 142
Ajouter ou modifier un numéro PAN (Permanent Account Number, numéro de compte permanent) 143
Modifier plusieurs numéros PAN (Permanent Account Number, numéros de comptes permanents) 143
Modifier plusieurs numéros de taxe sur les biens et services (GST) 144
Afficher une facture fiscale 144
Changer le vendeur enregistré vers ou depuis AWS Inde 145
AWS Support d'accès 147

Accompagnement de projets 147
Support technique 148
Support si tous vos projets et votre organisation sont fermés 148
Démarrez un essai Business Support+ 148
Surveillez votre projet 149
Surveillez votre projet à l'aide de AWS CloudTrail 150
CloudTrail À utiliser pour voir qui a modifié votre projet 150
Fermer un projet 153
Ce que vous devez savoir avant de clôturer votre projet 153
Pour clôturer un projet 154
Post-closure période 154
Réouverture de votre projet 155
Activer les fonctionnalités avancées 155
Que se passe-t-il lorsque vous activez les fonctionnalités avancées 155
Comptes de projet après avoir activé les fonctionnalités avancées 158
Comment va AWS Les paramètres changent-ils après avoir activé les fonctionnalités avancées ? 159
Puis-je tout de même créer un projet dans AWS Réglages après avoir activé les fonctionnalités avancées ? 160
Comment se préparer à activer les fonctionnalités avancées 160
Comment activer les fonctionnalités avancées 161
Après avoir activé les fonctionnalités avancées 162
Définissez un mot de passe utilisateur root 162
Gérer les membres du personnel 164
Modifier la source d'identité 166
Supprimer les politiques de l'organisation 167
Fermez votre compte dans AWS les paramètres 169
Ce que vous devez savoir avant de fermer votre compte de gestion 169
Fermer un projet 170
Fermez votre compte de gestion 170
Supprimez votre AWS ID de créateur 170
Inscrivez-vous à AWS (avancé) 172
Étape 1 : Créez votre compte 173
Étape 2 : (recommandé) Installez le AWS CLI 175
Étape 3 : (Recommandé) Configurez le AWS Serveur MCP 176
Connexe AWS services 176

Utilisation de l'utilisateur root 178
Accès à votre compte 178
Planifiez votre structure de gouvernance 179
Avantages de l'utilisation de plusieurs Comptes AWS 180
Quand l'utiliser AWS Organizations 182
Quand l'utiliser AWS Control Tower 189
Comprendre les modes de fonctionnement des API 189
Configurez votre compte 193
Créez ou mettez à jour l'alias de votre compte 194
Activer ou désactiver Régions AWS dans votre compte 194
Mettez à jour la facturation de votre Compte AWS 206
Mettre à jour l'adresse e-mail de l'utilisateur root (e-mail) 206
Mettre à jour le mot de passe utilisateur root 212
Mettez à jour votre Compte AWS name 213
Mettez à jour les contacts alternatifs de votre Compte AWS 218
Mettez à jour le contact principal de votre Compte AWS 227
Afficher les identifiants de votre compte 238
Résoudre les problèmes liés à votre compte 245
Problèmes liés à la création de compte 245
Problèmes liés à la fermeture du compte 246
Autres problèmes 248
Gérer des comptes en Inde 249
Créez un Compte AWS avec AWS Inde 250
Gérez les informations de vérification de vos clients 253
Fermez votre compte 258
Ce que vous devez savoir avant de fermer votre compte 259
Comment fermer votre compte 261
À quoi s'attendre après la fermeture de votre compte 265
Rouvrez votre compte 266
Ce que vous devez savoir avant de rouvrir votre compte 266
Comment rouvrir votre compte 267
À quoi s'attendre après la réouverture de votre compte 267
Préparez votre compte en vue de son utilisation après sa réouverture 268
Disponibilité dans les Régions 268
Sécurisez votre compte 269
Protection des données 270

AWS PrivateLink 271
Création du point de terminaison 272
Politiques relatives aux terminaux Amazon VPC 272
Politiques de point de terminaison 273
Gestion de l'identité et des accès 273
Public ciblé 274
Authentification par des identités 274
Gestion de l'accès à l'aide de politiques 276
AWS Gestion des comptes et IAM 278
Identity-based exemples de politiques 286
Utilisation de politiques basées sur l'identité 290
Résolution des problèmes 293
AWS politiques gérées 295
AWSAccountManagementReadOnlyAccess 296
AWSAccountManagementFullAccess 297
Mises à jour des politiques 298
Validation de conformité 299
Résilience 300
Sécurité de l'infrastructure 300
Surveillez votre compte 302
CloudTrail journaux 302
Informations relatives à la gestion des comptes dans CloudTrail 303
Comprendre les entrées du journal de gestion des comptes 304
Surveillance des événements liés à la gestion des comptes avec EventBridge 308
Événements liés à la gestion des comptes 308
Quotas 311
Historique de la documentation 314
..... cccxviii

Qu'est-ce qu'un Compte AWS?

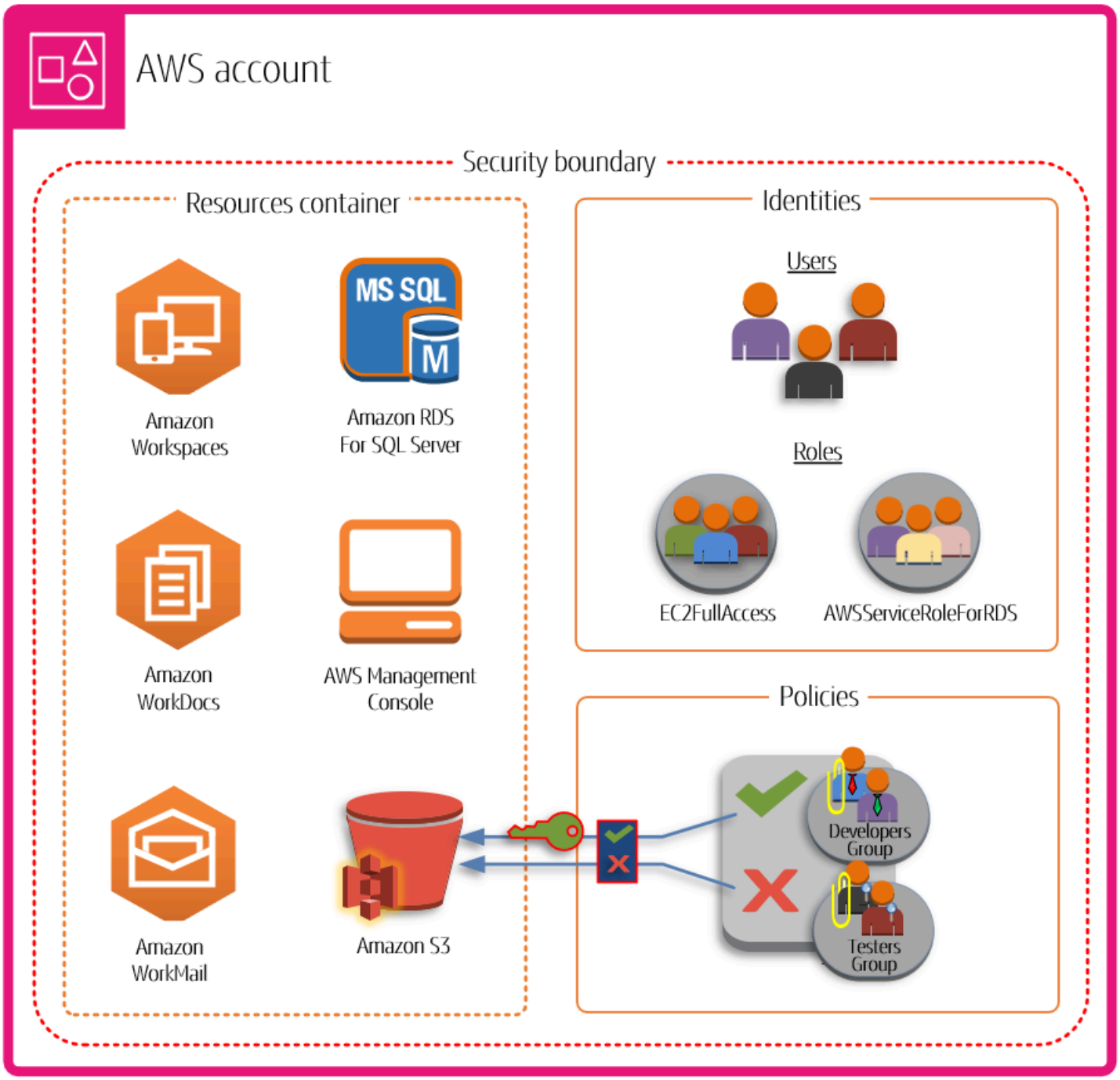
An Compte AWS représente une relation d'affaires officielle avec laquelle vous établissez AWS. Vous créez et gérez vos AWS ressources dans un Compte AWS, et votre compte fournit des fonctionnalités de gestion des identités pour l'accès et la facturation. Chacun Compte AWS possède un identifiant unique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

Lorsque vous vous inscrivez AWS, vous pouvez choisir entre S'inscrire pour AWS (nouveau) et S'inscrire pour AWS (avancé). Selon votre choix, vous avez accès à des projets Comptes AWS ou à des projets. Les projets contiennent Comptes AWS et les paramètres de partage avec d'autres collaborateurs. Pour de plus amples informations, veuillez consulter Comparez les options d'inscription.

Vos ressources et données cloud sont contenues dans un Compte AWS. Un compte fait office de 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 autoriser explicitement 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 hors production, aucun accès n'est autorisé entre ces environnements par défaut.

Comptes AWS constituent également un élément fondamental de l'accès aux AWS services. Comme le montre l'illustration suivante, an 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 compartiment Amazon Simple Storage Service (Amazon S3), une base de données Amazon Relational Database Service (Amazon RDS) et une instance Amazon Elastic Compute Cloud (Amazon EC2) sont tous des ressources. Chaque ressource est identifiée de manière unique par un Amazon Resource Name (ARN) qui inclut l'identifiant du compte qui contient ou possède la ressource.
- Limite de sécurité — A Compte AWS est également la limite de sécurité de base pour vos AWS ressources. Les ressources que vous créez dans votre compte sont mises à la disposition des utilisateurs qui disposent d'informations d'identification pour votre compte. Parmi les ressources clés 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 fonctionnalités Comptes AWS constitue 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 d'être adaptable 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 par lequel AWS les coûts sont répartis. De ce fait, l'utilisation de différents comptes pour différentes unités commerciales et groupes de charges de travail peut vous aider à suivre, contrôler, prévoir, budgétiser et rapporter plus facilement vos dépenses liées au cloud. Outre les rapports sur les coûts au niveau du compte, il dispose AWS également d'un support intégré permettant de consolider et de signaler les coûts sur l'ensemble de votre ensemble de comptes si vous choisissez de les utiliser AWS Organizations à un moment donné. Vous pouvez également utiliser les quotas de AWS service pour vous protéger contre un approvisionnement excessif et inattendu de AWS ressources et contre des actions malveillantes susceptibles d'avoir un impact considérable sur vos AWS coûts.
- Unité d'isolation — An 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 provisionnées au sein d'un compte sont logiquement isolées des ressources provisionnées 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 l'application, à une mauvaise configuration ou à des actions malveillantes. Si un problème survient au sein d'un compte, les impacts sur les charges de travail contenues dans d'autres comptes peuvent être réduits ou éliminés.
- Reproduisez vos charges de travail professionnelles : utilisez plusieurs comptes pour regrouper les charges de travail ayant un objectif commercial commun dans des comptes distincts. Vous pouvez ainsi 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.

C'est la première fois AWS utilisateur ?

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Si vous utilisez pour la première fois AWS, la première étape consiste à vous inscrire AWS. Vous pouvez soit créer un Compte AWS endroit où vous avez un contrôle total sur la configuration de votre compte et où votre contenu est stocké, ce qui est requis pour les charges de travail réglementées telles que HIPAA ou FedRAMP, soit créer avec des paramètres par défaut préconfigurés. Comptes AWS Pour savoir quelle inscription vous convient le mieux, consultezComparez les options d'inscription.

Pour obtenir des instructions détaillées sur la configuration d'un nouveau compte dans lequel vous avez le contrôle total de la configuration initiale, consultezInscrivez-vous pour AWS (avancé).

Pour obtenir des instructions détaillées sur la configuration d'un nouveau compte dans le cadre duquel des comptes sont AWS créés avec des paramètres par défaut préconfigurés, consultez. Inscrivez-vous pour AWS (nouveau)

Prise en charge de AWS Gestion du compte

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 Console de gestion AWS. Pour plus d'informations, voir Exemple : création d'un dossier d'assistance pour le compte et la facturation.

Autre AWS resources

- 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. Inclut également des liens vers d'autres ressources utiles, telles que des forums, des FAQ techniques, l'état d'un service et AWS Trusted Advisor.
- AWS Support : page Web principale contenant des informations sur le AWS support, un canal d'assistance personnalisé et 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.

Comparez les options d'inscription

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

En vous inscrivant AWS, vous accédez au cloud le plus complet et le plus largement adopté au monde. Nous offrons le plus grand choix de capacités et d'expertise innovantes en matière de cloud et d'IA, sur l'infrastructure mondiale la plus étendue, avec une sécurité, une fiabilité et des performances de pointe.

Il existe deux façons de s'inscrire à AWS. Si vous souhaitez contrôler totalement la configuration de votre compte et l'emplacement de stockage de votre contenu, ou si vous avez des charges de travail réglementées telles que HIPAA, FedRAMP, utilisez. Inscrivez-vous pour AWS (avancé) Si vous êtes un nouvel utilisateur et que vous souhaitez utiliser un identifiant que vous possédez déjà pour vous connecter AWS et créer un AWS environnement avec des paramètres par défaut préconfigurés dans select Régions AWS, utilisez. Inscrivez-vous pour AWS (nouveau)

Pris en charge Services AWS pour Inscrivez-vous pour AWS (nouveau)

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Lorsque vous utilisez Sign up for AWS (new), vous avez accès au niveau gratuit. Le niveau gratuit donne accès à certains AWS services. Vous pouvez passer à un forfait payant pour accéder à des AWS services et fonctionnalités supplémentaires. Pour savoir comment mettre à jour votre compte, consultezMettez à jour votre compte dans AWS Settings.

Tous les AWS services ne sont pas disponibles pour s'inscrire AWS (nouveau). Si un service ne figure dans aucune des listes suivantes ou possède une fonctionnalité non prise en charge, vous

devez créer un compte à l'aide de Inscrivez-vous pour AWS (avancé) ouActiver le mode avancé AWS fonctionnalités.

Services AWS inclus dans le niveau gratuit de notre nouveau AWS expérience

Les AWS services suivants sont inclus dans le niveau gratuit d'inscription à AWS (nouveau). Multi-Region ou Les fonctionnalités interrégionales ne sont prises en charge pour aucun service. Pour plus d'informations, consultez Régions AWS pour vos projets.

- Amazon API Gateway
- Amazon Athena
- Amazon AppFlow
- AWS App2Container
- IA augmentée d'Amazon
- Amazon Bedrock
- Amazon Bedrock Agent Core
- Amazon CloudFront
  - Lambda @Edge n'est pas pris en charge.
- Amazon CloudWatch
- Amazon CloudWatch Logs
- Amazon CodeGuru Profiler
- Amazon Cognito
- Amazon Cognito Sync
- Amazon DynamoDB
- Amazon DataZone
- Amazon Elastic Container Registry (ECR)
- EC2 Image Builder
- Amazon EKS Anywhere
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
  - Le bloc de capacité d'achat et l'extension du bloc de capacité d'achat ne sont pas pris en charge.

- Amazon Elastic Container Registry Public
- Amazon Elastic Container Service
- Amazon Elastic Kubernetes Service
- Amazon Elastic File System
- Amazon ElastiCache
- Amazon EventBridge
- Amazon Lex
- Amazon Lightsail
- Amazon Location Service
- Amazon Managed Service for Prometheus
- Amazon Managed Workflows for Apache Airflow
- Amazon MQ
- Amazon OpenSearch Service
- Amazon Polly
- Amazon Quick
  - Seuls Amazon Quick Free ou Quick Plus sont pris en charge. Pour plus d'informations, consultez les tarifs Amazon Quick.
- Amazon Rekognition
- Amazon Relational Database Service
- Amazon Route 53
- Amazon SageMaker
- Amazon SageMaker AI
- Amazon SageMaker Unified Studio
- Amazon Simple Email Service
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- Amazon Simple Storage Service
  - Amazon S3 Access Grants n'est pas pris en charge.
- Amazon Simple Workflow Service
- Amazon Verified Permissions

- Amazon Virtual Private Cloud
- Amazon Aurora
- Amazon Aurora DSQL
- AWS Amplify
- AWS AppConfig
- AWS AppSync
- Application Autoscaling
- AWS Transform MGN
- AWS Artifact
  - L'addendum (HIPAA) AWS Business Associate, l'addendum (HIPAA) AWS Organizations Business Associate, l'addendum à la règle 17a-4 de la SEC et l'addendum AWS à la règle 18a-6 de la SEC ne sont pas pris en charge. AWS
- AWS B2B Échange de données
- Agent AWS Backint
- AWS Backup
- AWS Batch
- AWS Billing and Cost Management
  - Utilisez AWS les paramètres pour configurer votre facturation, créer des limites de dépenses afin de contrôler vos coûts, ainsi que pour récupérer et payer les factures. Vous utilisez Billing and Cost Management pour créer des budgets, analyser et optimiser vos coûts. Pour plus d'informations, consultez la section Utilisation de la console Billing and Cost Management avec notre nouvelle AWS expérience.
- AWS Budgets
- AWS Certificate Manager
  - AWS Les certificats publics exportables de Certificate Manager ne sont pas pris en charge.
- API de commande du Cloud AWS
- AWS Cloud Map
- AWS Cloud9
- AWS CloudFormation
- AWS CloudShell
- AWS CloudTrail

- AWS CodeArtifact
- AWS CodeCommit
- AWS CodeDeploy
- AWS CodePipeline
- Optimiseur de calcul AWS
- AWS Config
- AWS Console Mobile Application
- AWS Cost Explorer
- AWS Data Pipeline
- AWS Transfert de données
- AWS DataSync
- AWS Directory Service
- AWS Elastic Beanstalk
- AWS End User Messaging Social
- Résolution des entités AWS
- AWS Glue
- AWS Health
- Gestion des identités et des accès AWS
- AWS IoT
  - AWS Greengrass n'est pas pris en charge.
- AWS IoT Défenseur de l'appareil
- AWS IoT Gestion des appareils
- AWS IoT SiteWise
- AWS IoT TwinMaker
- AWS Key Management Service
- AWS Lake Formation
- AWS Lambda
  - Lambda @Edge n'est pas pris en charge.
- AWS Launch Wizard
- AWS License Manager

- Console de gestion AWS
- AWS Marketplace
  - Bedrock et Free uniquement.
- AWS Network Manager
- AWS Payment Cryptography
- AWS PrivateLink
- AWS Resource Access Manager (RAM)
- Explorateur de ressources AWS
- Groupes de ressources AWS
- Contrôleur Route 53 Amazon Application Recovery (ARC)
- AWS SDK et outils
- AWS Secrets Manager
- AWS Security Token Service
- AWS Serverless Application Repository
- Service Quotas
- AWS Signer
- AWS Step Functions
- AWS Support
- AWS Systems Manager
- Gestionnaire de systèmes AWS pour SAP
- Notifications des utilisateurs AWS
  - User-configured les opérations de configuration des notifications et des notifications gérées ne sont pas prises en charge. Pour plus d'informations, voir Qu'est-ce que les notifications AWS utilisateur ?
- AWS WAF
  - AWS Shield n'est pas pris en charge.
- AWS Well-Architected Tool
- AWS X-Ray
- AWS CodeBuild
- Elastic Load Balancing

- AWS SQL Workbench
- Amazon OpenSearch Service sans serveur
- Amazon Timestream

Pour connaître la politique qui contrôle l'accès aux services de niveau gratuit, consultezPolitiques de contrôle des services pour le niveau gratuit pour les projets.

Services AWS inclus dans le plan payant de notre nouveau AWS expérience

Les services suivants sont disponibles pour s'inscrire AWS (nouveau) si vous avez un forfait payant. Pour plus d'informations, consultezMettez à jour votre compte dans AWS Settings. Multi-Region ou Les fonctionnalités interrégionales ne sont prises en charge pour aucun service. Pour plus d'informations, consultez Régions AWS pour vos projets.

- Amazon DevOps Guru
- Amazon DocumentDB (compatible avec MongoDB)
- Amazon EMR
- Amazon Forecast
- Amazon Glacier
- Amazon Kinesis
- Amazon Kinesis Data Streams
- Amazon Data Firehose
- Amazon Kinesis Video Streams
- Amazon Managed Blockchain
- Amazon Managed Streaming for Apache Kafka
- Amazon MemoryDB
- Amazon Neptune
- Amazon Personalize
- Amazon Redshift
- S3 Glacier Deep Archive
- Amazon Textract

- Amazon Transcribe
- Amazon Translate
- AWS AppFabric
- AWS Data Exchange
- AWS End User Messaging SMS
- AWS Fault Injection Service
- AWS Firewall Manager
- AWS Network Firewall
- AWS Agent de sécurité
- AWS Storage Gateway
- DevOps Agent

Pour connaître la politique qui contrôle l'accès aux services du forfait payant, consultezPolitiques de contrôle des services pour le plan payant pour les projets.

Services AWS non pris en charge pour notre nouveau AWS expérience

Les AWS services suivants ne sont pas pris en charge pour notre nouvelle AWS expérience, sauf si vousActiver le mode avancé AWS fonctionnalités. Ces AWS services ne sont pas nécessaires pour les nouveaux développeurs ou les petites équipes. Certains de ces services sont automatiquement activés pour votre compte et gérés par AWS. Pour plus d'informations, consultez Comparez les fonctionnalités des options d'inscription.

- Alexa for Business
- Alexa Top Sites
- Alexa Web Information Service
- Amazon Braket
- Amazon Chime
- Amazon Chime Business Calling, un service vendu par AMCS LLC
- Amazon Chime Appelez-moi
- Amazon Chime Call Me, un service vendu par AMCS LLC
- Amazon Chime Dial In, un service vendu par AMCS LLC
- Amazon Chime Dialin

- Fonctionnalités d'Amazon Chime
- Kit SDK Amazon Chime
- Amazon Chime Services
- SMS Amazon Chime
- Amazon Chime Voice Connector, un service vendu par AMCS LLC
- Amazon Cloud Directory
- Amazon CloudSearch
- Amazon CodeWhisperer
- Amazon Connect Customer
- Profils des clients Amazon Connect
- Identifiant vocal du client Amazon Connect
- AWS Deadline Cloud
- Amazon Detective
- Amazon Elastic Inference
- Amazon Elastic Transcoder
- Amazon FinSpace
- Flotte flexible Amazon
- Amazon Fraud Detector
- Amazon FSx
- GameLift Serveurs Amazon
- Amazon GameLift Streams
- Amazon GameSparks
- Amazon GuardDuty
- AWS HealthOmics
- Amazon Inspector Classic
- Amazon Interactive Video Service
- Chat Amazon IVS
- Amazon Kendra
- Amazon Keyspaces (pour Apache Cassandra)
- Kiro

- Amazon Macie
- Amazon Managed Grafana
- Amazon Mechanical Turk
- Récompenses pour les employés d'Amazon Mechanical Turk
- Amazon Mobile Analytics
- Amazon Monitron
- Amazon Nimble Studio
- OpenSearch Service d'ingestion de services Amazon
- Amazon Q
- Amazon Q Business
- Amazon Q Developer
- Amazon Quantum Ledger Database (Amazon QLDB)
- Amazon S3 sur Outposts
- Amazon SageMaker Ground Truth
- Amazon Security Lake
- Amazon Sumerian
- Amazon WorkDocs
- Amazon WorkSpaces
- WorkSpaces Instances Amazon
- WorkSpaces Applications Amazon (Amazon WorkSpaces Applications)
- Amazon WorkSpaces Thin Client
- WorkSpaces Site Web d'Amazon
- Amazon WorkLink
- Amazon WorkMail
- AWS Profileur des coûts d'application
- AWS Clean Rooms
- AWS Studio d'applications
- AWS Application Discovery Service
- AWS Audit Manager
- AWS Billing Conductor

- AWS CloudHSM
- AWS Client VPN
- AWS Réseau WAN dans le cloud
- AWS Control Tower
- AWS Service de Migration de Base de Données
- AWS DeepRacer
- AWS Device Farm
- AWS Direct Connect
- Reprise après sinistre AWS Elastic
- AWS Elemental Live
- AWS Elemental MediaConnect
- AWS Elemental MediaConvert
- AWS Elemental MediaLive
- AWS Elemental MediaPackage
- AWS Elemental MediaStore
- AWS Elemental MediaTailor
- AWS Global Accelerator
- AWS Ground Station
- AWS HealthImaging
- AWS IAM Identity Center
- AWS Identity and Access Management Access Analyzer
- AWS Interconnecter
- AWS IoT Événements
- AWS IoT FleetWise
- AWS IoT RoboRunner
- AWS Mainframe Modernization
- AWS Migration Hub
- AWS Migration Hub Refactor Spaces
- AWS Modular Data Center
- AWS OpsWorks

- AWS Organizations
- AWS Outposts
- AWS Parallel Computing Service
- AWS Partner Network
- Calculateur de tarification AWS
- Autorité de certification privée AWS
- AWS Proton
- AWS re:Post privé
- AWS Resilience Hub
- AWS RoboMaker
- AWS Tissu RTB
- AWS Security Hub
- Réponse aux incidents de sécurité AWS
- AWS Service Catalog
- AWS Shield
- AWS SimSpace Weaver
- AWS Snowball
- AWS Supply Chain
- Générateur de réseau de télécommunications AWS
- AWS Transform
- AWS Transfer Family
- AWS Transit Gateway
- AWS Trusted Advisor
- Accès vérifié par AWS
- Site-to-Site VPN
- Amazon VPC Lattice
- AWS Wickr
- Amazon CodeCatalyst
- Amazon Comprehend Medical
- Télécommunications de conférence (service vendu par AMCS LLC)

- Contact Center Telecommunications (service vendu par AMCS LLC)
- Centre d'appels Telecommunications Korea
- Centre de contact Telecommunications Afrique du Sud
- DynamoDB Accelerator
- Service Amazon Elastic VMware
- Oracle Database@AWS
- Red Hat OpenShift Service on AWS
- AWS App Runner

Considérations relatives au choix du mode d'inscription à AWS

Tenez compte des points suivants avant de choisir votre méthode d'inscription. Vous pouvez activer toutes les AWS fonctionnalités de votre compte si nécessaire.

- Si vous avez des exigences spécifiques en matière de produits, telles que des charges de travail réglementées incluant les normes HIPAA ou FedRAMP, n'utilisez pas notre nouvelle expérience. AWS
- Votre contenu sera stocké dans une région désignée qui est sélectionnée en fonction de vos coordonnées.
- La nouvelle AWS expérience vous permet de commencer à créer plus facilement sans créer d' AWS autorisations. Si vous avez besoin d'un contrôle précis de vos utilisateurs ou d'autorisations basées sur les rôles, n'utilisez pas l'option S'inscrire pour AWS (nouveau).
- Si vous avez besoin de configurations de paiement spécifiques à un compte définies par AWS, également connues sous le nom de facturation selon les termes nets, n'utilisez pas l'option S'inscrire pour AWS (nouveau).
- Si vous avez besoin d'accéder à l'ensemble des AWS services, n'utilisez pas l'option S'inscrire pour AWS (nouveau). Pour plus d'informations, consultez Pris en charge Services AWS pour Inscrivez-vous pour AWS (nouveau).

Comparez les fonctionnalités des options d'inscription

Le tableau suivant compare AWS les exigences générales prises en charge pour s'inscrire pour AWS (nouveau) ou pour s'inscrire pour AWS (avancé). Si une fonctionnalité n'est pas répertoriée dans ce tableau ou décrite dansComparaison de la gestion des accès, elle est disponible. Vous pouvez

activer les fonctionnalités avancées de votre compte si vous avez besoin de fonctionnalités non prises en charge. Pour plus d'informations, consultez Activer le mode avancé AWS fonctionnalités.

Fonctionnalité	Inscrivez-vous à AWS (nouveau)	Inscrivez-vous à AWS (avancé)
Rejoignez le réseau de AWS partenaires	Non	Oui
Création d'un contrat de services professionnels	Non	Oui
Souscrivez un accord d'entreprise avec AWS	Non	Oui
Souscrivez un abonnement à AWS Skill Builder Team	Non	Oui
Collaborez avec un partenaire AWS de formation	Non	Oui
Gagnez des crédits supplémentaires avec AWS Activate	Non	Oui
Utilisez AWS Marketplace	Non	Oui
Désignez votre AWS compte comme étant conforme à la loi HIPAA ou à la SEC	Non	Oui
Sélectionnez une ressource spécifique Région AWS pour créer vos ressources régionales	Non Pour plus d'informations, consultezRégions AWS pour vos projets.	Oui
Accédez à une région optionnelle	Non	Oui
IAM Access Analyzer	Non	Oui
Sign-in politiques d'accès	Non	Oui
Fixez des limites de dépenses pour vos comptes	Oui	Non

Fonctionnalité	Inscrivez-vous à AWS (nouveau)	Inscrivez-vous à AWS (avancé)
Savings Plans	Non	Oui
Inscription automatique au hub d'optimisation des coûts pour le plan payant	Oui	Non
Inscription automatique à AWS Organizations	Oui	Non
Inscription automatique à IAM Identity Center	Oui	Non
S'inscrire automatiquement au gestionnaire de rôles IAM	Oui	Non
Couleurs du compte console	Non	Oui
Utilisation de la AWS Console Mobile Application	Non	Oui
Désactiver la prise en charge des consoles multi-sessions	Non	Oui. Si vous vous reconnectez à l'aide d'un identifiant Builder, le support multisession sera automatiquement activé.

Comparaison de la gestion des accès

Lorsque vous utilisez notre nouvelle AWS expérience, elle AWS crée des valeurs par défaut préconfigurées pour vous aider à commencer à créer. Vos AWS ressources sont organisées en projets. Un projet contient un compte Compte AWS, appelé compte de projet, et des paramètres de partage avec d'autres collaborateurs. Si vous utilisez le plan payant, votre projet peut également avoir un coût mensuel avant impôts défini, appelé limite de dépenses. Tous les projets que vous possédez constituent votre organisation, que vous contrôlez via votre compte de gestion dans AWS les paramètres. Cette organisation est identique à une AWS organisation ; toutefois, AWS elle gère certains aspects de cette organisation en votre nom.

AWS gère les éléments suivants de votre AWS organisation :

- Politiques de gestion de l'organisation. Lorsque vous utilisez notre nouvelle AWS expérience, AWS gère les politiques de gestion de l'organisation, y compris les politiques de contrôle des ressources (RCP) et les politiques de contrôle des services (SCP). Si vous souhaitez créer le vôtre, utilisez S'inscrire pour AWS (avancé).
- Rôles d'accès humain. Un rôle d'accès humain est un rôle qui accorde des autorisations spécifiques à un être humain. AWS vous donne, à vous et aux membres de votre équipe, un accès administrateur à vos projets. En tant que propriétaire du projet, vous pouvez ajouter et supprimer des membres de l'équipe. Pour plus d'informations, consultez Invitez les membres de l'équipe à collaborer AWS Settings. Vous ne créez pas d'utilisateur root. Votre AWS Builder ID est propriétaire de vos comptes de projet et non de l'adresse e-mail de l'utilisateur root, et cela ne change pas lorsque vous activez les fonctionnalités avancées. Vous pouvez créer des rôles IAM et des utilisateurs IAM si nécessaire, mais ils ne peuvent être utilisés que pour l'accès par programmation, et non pour l'accès à la console.

Chaque projet est doté d'une implémentation de sécurité gérée qui permet de le développer facilement en toute confiance. Par défaut, toute application ou tout code de votre projet a accès à toutes les AWS ressources de ce même projet. Il n'est pas nécessaire d'effectuer une configuration d'accès supplémentaire.

AWS les ressources des différents projets ne peuvent pas accéder les unes aux autres, sauf si vous activez l'accès entre projets pour certaines ressources. Par exemple, vous pouvez créer une fonction Lambda dans un projet, puis l'invoquer à l'aide d'une API dans un autre projet. C'est ce que l'on appelle une intégration entre comptes. Pour plus d'informations, consultez la section Cross-accountIntégrations Lambda. Tant que les deux projets sont détenus par le même compte de gestion, cela est pris en charge.

Par défaut, votre projet ne fournit aucun accès externe à aucune ressource. Vous devez configurer AWS les ressources pour autoriser l'accès public. Vous pouvez effectuer les opérations suivantes :

- Créez un compartiment S3 public pour héberger un site Web ou des fichiers statiques simples. Pour plus d'informations, consultez Getting started with Amazon S3.
- Créez une API API Gateway qui servira de porte d'entrée à votre application. Pour plus d'informations, voir Création d'une API HTTP.
- Créez une instance EC2 avec une adresse IP publique pour permettre la communication entre vos instances et Internet. Pour plus d'informations, consultez Lancer votre première instance EC2.

- Créez une CloudFront distribution pour diffuser votre contenu Web statique et dynamique, tel que les fichiers .html, .css, .js et les fichiers image, à vos utilisateurs. Pour plus d'informations, consultez la section Mise en route avec CloudFront.
- Créez une URL de fonction Lambda pour fournir un point de terminaison HTTP simple et direct accessible au public pour une fonction Lambda. Assurez-vous que votre fonction Lambda dispose des autorisations appropriées. Pour plus d'informations, consultez Création d'une URL de fonction et Modèle de sécurité et d'authentification pour les URL de fonction Lambda.
- Utilisez une combinaison de ces AWS mécanismes ou d'autres.

En outre, lorsque vous activez des fonctionnalités avancées, vous avez accès à encore plus de mécanismes pour fournir un accès externe à vos ressources.

Gérez votre Comptes AWS

Vous gérez votre Comptes AWS en fonction du type de produit que AWS vous utilisez. Le tableau suivant indique où trouver la documentation pour chaque tâche de gestion.

Sous-tâche	Inscrivez-vous pour AWS (nouveau)	Inscrivez-vous pour AWS (avancé)
S'inscrire	Inscrivez-vous pour AWS (nouveau)	Inscrivez-vous pour AWS (avancé)
Création d'un compte	Créez un projet dans AWS Settings	Inscrivez-vous pour AWS (avancé)
Fermer un compte	Fermer un projet dans AWS Settings	Fermez un Compte AWS
Mettez à jour votre mot de passe	Mettez à jour votre mot de passe dans AWS Settings	Mettre à jour le mot de passe utilisateur root
Enregistrer les appareils MFA	Gérez l'authentification multifactorielle (MFA) dans AWS Settings	Étape 3 : (Recommandé) Configurez le AWS Serveur MCP

Sous-tâche	Inscrivez-vous pour AWS (nouveau)	Inscrivez-vous pour AWS (avancé)
Changez votre adresse e-mail	Changez votre adresse e-mail dans AWS Settings	Mettez à jour le Adresse e-mail de l'utilisateur racine
Changez votre nom	Gérez votre nom ou votre surnom dans AWS Settings	Mettez à jour votre Compte AWS name
Mettre à jour les informations de contact	Modifiez vos informations de contact dans AWS Settings	Mettez à jour le contact principal de votre Compte AWS
Mettre à jour les contacts alternatifs	Non applicable	Mettez à jour les contacts alternatifs de votre Compte AWS
Gérer la facturation	Gérez votre mode de paiement dans AWS Settings	Mettez à jour la facturation de votre Compte AWS
Gérer les informations fiscales	Gérez l'enregistrement fiscal dans AWS Settings	Gérez vos paiements
Activer ou désactiver Régions AWS	Non applicable. Vous ne pouvez pas modifier votre Région AWS.	Activer ou désactiver Régions AWS dans votre compte
Afficher les identifiants de compte	Non applicable	Afficher Compte AWS identifiants
Créer un alias de compte	Non applicable	Créez un Compte AWS alias

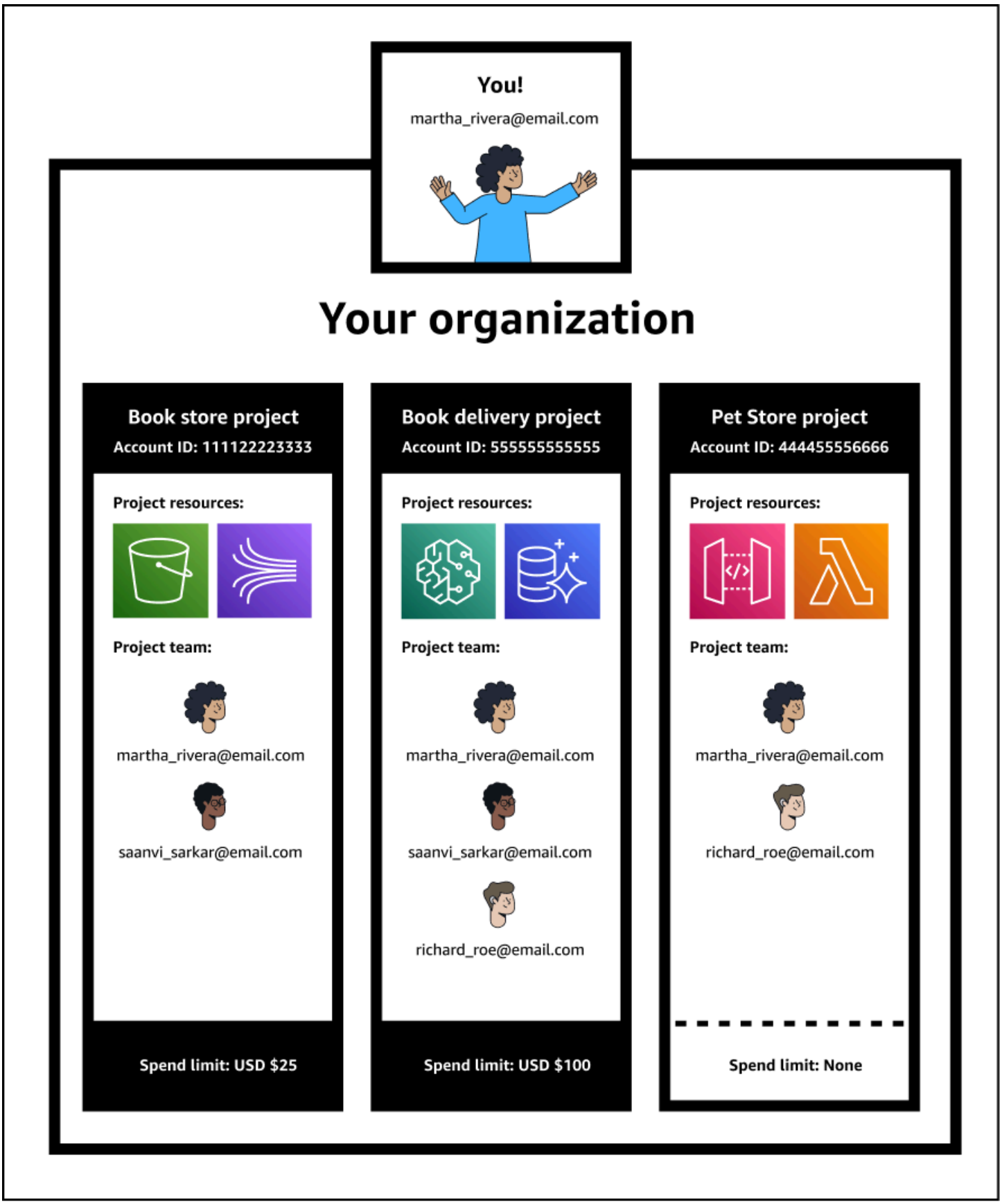
Sous-tâche	Inscrivez-vous pour AWS (nouveau)	Inscrivez-vous pour AWS (avancé)
Améliorez votre compte	Mettez à jour votre compte dans AWS Settings	Plans de niveaux gratuits
Créer une limite de dépenses	Créez une limite de dépenses dans AWS Settings	Non applicable
Mettre à jour une limite de dépenses	Mettre à jour une limite de dépenses dans AWS Settings	Non applicable
Supprimer une limite de dépenses	Supprimer une limite de dépenses dans AWS Settings	Non applicable
Inviter des membres de l'équipe	Invitez les membres de l'équipe à collaborer AWS Settings	Identités IAM
Basculer entre les projets	Basculer entre les projets	Multi-session soutien
Connect un outil de codage basé sur l'IA	Connectez un outil de codage basé sur l'IA	Non applicable
Supprimer toutes les sessions	Supprimer toutes les sessions dans AWS Settings	Non applicable
Refuser l'utilisation des données de l'IA	Désactivez l'utilisation de votre contenu pour améliorer le service dans AWS Settings	Politiques de désabonnement aux services d'IA

Sous-tâche	Inscrivez-vous pour AWS (nouveau)	Inscrivez-vous pour AWS (avancé)
Demandez vos données	Demandez votre AWS Données d'identification du constructeur	Demandez vos données
Supprimer votre AWS profil	Fermez votre compte dans AWS Settings	Fermez un Compte AWS
Gérer des comptes en Inde	Gérez des comptes en Inde dans AWS Settings	Gérer des comptes en Inde
Création d'un utilisateur administrateur	Non applicable	Inscrivez-vous pour AWS (avancé)
Planifiez la structure de gouvernance de votre compte	Non applicable	Planifiez votre Compte AWS structure de gouvernance

Inscrivez-vous pour AWS (nouveau)

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Lorsque vous utilisez Sign up for AWS (new), vous créez un AWS environnement préconfiguré qui vous permet d'utiliser un identifiant que vous possédez déjà, tel que Google, ou GitHub pour accéder à vos AWS ressources. Vos ressources sont organisées en projets. Un projet contient un Compte AWS et des paramètres à partager avec d'autres collaborateurs. Si vous utilisez le plan payant, votre projet peut également avoir un coût mensuel avant impôts défini, appelé limite de dépenses. Tous les projets que vous possédez constituent votre organisation. Vous gérez votre organisation, accédez à vos projets et ajoutez des membres à l'équipe dans AWS les paramètres.


You!
martha_rivera@email.com
Your organization
Book store project
Account ID: 111122223333
Project resources:
Project team:
martha_rivera@email.com
saanvi_sarkar@email.com
Spend limit: USD $25
Book delivery project
Account ID: 555555555555
Project resources:
Project team:
martha_rivera@email.com
saanvi_sarkar@email.com
richard_roe@email.com
Spend limit: USD $100
Pet Store project
Account ID: 444455556666
Project resources:
Project team:
martha_rivera@email.com
richard_roe@email.com
Spend limit: None

Lorsque vous vous inscrivez pour AWS utiliser Sign up for AWS (new), crée AWS également un ID de constructeur AWS compte, qui est un profil personnel qui vous représente en tant qu'individu. Vous ne pouvez en avoir qu'une ID de constructeur AWS pour chaque adresse e-mail. Si vous en avez créé un ID de constructeur AWS mais que vous n'en avez pas créé Compte AWS, certains paramètres ont peut-être déjà été définis pour vous et vous devrez les modifier ultérieurement.

Pour plus d'informations sur Sign up for AWS (new), consultez la documentation suivante :

- Comparez les options d'inscription
- Pris en charge Services AWS pour Inscrivez-vous pour AWS (nouveau)

Inscrivez-vous en utilisant S'inscrire pour AWS (nouveau)

Lorsque vous vous inscrivez AWS, nous pouvons vous demander des informations de paiement. Notre processus de vérification permet de conserver 1 USD (ou équivalent) pendant 3 à 5 jours afin de vérifier votre compte et de prévenir les fraudes. Vous n'aurez aucun frais à payer tant que vous ne passerez pas à un forfait payant. Vous pouvez gérer votre mode de paiement ou fermer vos comptes à tout moment via AWS les paramètres. En outre, lorsque vous vous inscrivez AWS, il se peut que vous ne soyez pas éligible au niveau gratuit. Dans ce cas, vous devrez fournir vos informations de paiement et vous serez placé sur le plan payant. Lorsque vous optez pour le plan payant, vous pouvez définir des limites de dépenses pour fonctionner dans le cadre d'un budget prévisible et contrôlé.

Inscrivez-vous pour bénéficier de AWS (nouvelles) aides en utilisant Google GitHub, Apple ou Amazon pour votre compte. Si vous êtes déjà connecté à un compte Google dans votre navigateur, ce compte sera utilisé lors de votre inscription AWS.

Pour vous inscrire à AWS en utilisant Sign up for AWS (nouveau)

1. Ouvrez la AWS page d'inscription.
2. Entrez votre e-mail ou choisissez un identifiant tel que Google GitHub, Apple ou Amazon.
3. Si vous utilisez un identifiant que vous possédez déjà, vous serez redirigé vers l'identifiant de votre fournisseur. Une fois connecté, vous serez redirigé pour vous AWS inscrire.
4. Entrez votre nom et choisissez Continuer.

   Ce nom est communiqué aux membres de l'équipe lorsque vous leur donnez accès à vos projets.

5. Vérifiez l'e-mail associé à votre identifiant en saisissant un code de vérification. Lorsque vous avez vérifié votre adresse e-mail, choisissez Continuer.

   Cet e-mail est partagé avec les membres de l'équipe lorsque vous leur donnez accès à vos projets.

6. Entrez un mot de passe sécurisé pour votre compte et 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.

7. Entrez vos coordonnées et choisissez Continuer.
8. AWS attribuera un nouveau nom à votre premier projet de Régions AWS l'un des trois. Pour plus d'informations, consultez Régions AWS pour vos projets. Vous pouvez modifier le nom à tout moment.

Vous pouvez désormais accéder au Console de gestion AWS. Pour accéder aux AWS paramètres, choisissez Gérer les projets dans le Console de gestion AWS. Dans AWS les paramètres, vous pouvez inviter des membres de l'équipe, créer de nouveaux projets et modifier vos paramètres de facturation et autres.

Étapes suivantes

Une fois inscrit AWS, vous pouvez connecter un outil de codage basé sur l'IA, ajouter des membres à l'équipe pour collaborer et, si vous avez un forfait payant, créer une limite de dépenses.

- Connectez un outil de codage basé sur l'IA
- Invitez les membres de l'équipe à collaborer AWS Settings
- Créez une limite de dépenses dans AWS Settings

Utilisation AWS Settings

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

AWS Les paramètres vous permettent de gérer vos projets et d'y accéder. AWS Les paramètres sont disponibles lorsque vous vous inscrivez à l'aide de S'inscrire pour AWS (nouveau). Vous pouvez utiliser AWS les paramètres pour effectuer les opérations suivantes :

- Créez des projets qui vous appartiennent et accédez-y. Pour de plus amples informations, veuillez consulter Créez un projet dans AWS Settings.
- Accédez aux projets qui ont été partagés avec vous.
- Invitez les membres de l'équipe à collaborer sur vos projets. Pour de plus amples informations, veuillez consulter Invitez les membres de l'équipe à collaborer AWS Settings.
- Passez d'un projet à l'autre. Pour de plus amples informations, veuillez consulter Basculer entre les projets.
- Gérez votre mode de paiement. Pour de plus amples informations, veuillez consulter Gérez votre mode de paiement dans AWS Settings.
- Passez du niveau gratuit à un plan payant. Pour de plus amples informations, veuillez consulter Mettez à jour votre compte dans AWS Settings.
- Gérez les limites de dépenses pour vos projets. Pour de plus amples informations, veuillez consulter Créez une limite de dépenses dans AWS Settings.
- Consultez vos informations de facturation. Pour de plus amples informations, veuillez consulter Consultez vos informations de facturation dans AWS Settings.
- Gérez les informations de votre profil. Pour plus d'informations, consultez Gérez votre nom ou votre surnom dans AWS Settings, Changez votre adresse e-mail dans AWS Settings et Modifiez vos informations de contact dans AWS Settings.
- Gérez vos paramètres de sécurité et vos préférences de connexion. Pour plus d'informations, consultez Mettez à jour votre mot de passe dans AWS Settings et Gérez l'authentification multifactorielle (MFA) dans AWS Settings.

Lorsque vous gérez les informations de votre profil ou vos paramètres de sécurité, vous êtes redirigé vers le ID de constructeur AWS hub. ID de constructeur AWS Le vôtre est créé lorsque vous utilisez S'inscrire pour AWS (nouveau). Pour plus d'informations, voir Qu'est-ce que c'est ID de constructeur AWS ? .

Connectez un outil de codage basé sur l'IA

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Vous pouvez fournir à votre outil de codage IA l'accès à votre projet et installer l'Agent Toolkit, qui regroupe la configuration du serveur AWS MCP et un ensemble de compétences d'agent sélectionnées. Cela permet à votre outil de codage d'IA de créer et de gérer AWS des ressources en votre nom.

Considérations relatives à la connexion de votre outil de codage à votre projet

- Vous pouvez connecter des outils de codage IA à un projet que vous possédez ou à un projet qui a été partagé avec vous.
- Lorsqu'un outil de codage basé sur l'IA ou un agent local crée AWS des ressources, vous en êtes toujours responsable. Cela inclut la sécurité adéquate de vos ressources, telle que définie par le modèle de responsabilité partagée, et tous les frais pouvant découler de ces ressources, qu'ils soient comptabilisés dans le plan gratuit ou facturés dans le plan payant.
- Vous êtes responsable de toutes les actions que votre outil de codage d'IA prend en votre nom dans le cadre de vos projets.
- Pour consulter une ressource créée par votre agent, accédez à la console de service correspondant à ce service.
- Les informations d'identification que vous générez sont destinées à être utilisées par les AWS CLI AWS outils pour et PowerShell les AWS kits SDK. Les outils externes peuvent ne pas être pris en charge. L'accès à vos ressources est valide pendant 12 heures. Utilisez la commande suivante pour renouveler vos informations d'identification :

```
aws login --profile profile-name
```

Remplacez-le *profile-name* par le nom de profil que vous avez choisi lors de la configuration initiale. La commande ouvre automatiquement votre navigateur par défaut. Vous devrez choisir le nom de votre projet pour terminer le processus de connexion. AWS peut renouveler vos informations d'identification pendant 90 jours. Après 90 jours, vous devrez à nouveau autoriser l'accès dans une fenêtre de navigateur.

Connectez votre outil de codage IA à votre projet

Chaque projet possède son propre ensemble d'informations d'identification que les outils de codage IA peuvent utiliser pour créer et gérer AWS des ressources en votre nom.

Console de gestion AWS

Pour connecter votre outil de codage IA à votre projet à l'aide du AWS console

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez le projet auquel vous souhaitez accéder.
3. Dans la barre de navigation en haut à droite, choisissez Créer et gérer une infrastructure cloud.
4. Choisissez Utiliser vos AWS informations d'identification avec les outils de codage IA.
5. Choisissez Copier l'invite de l'agent et saisissez-la dans votre agent de codage.

   Cela crée une invite qui partage un fichier de pilotage avec votre agent de codage AI. Le fichier de pilotage accède à un script AWS qui établit la connexion entre les informations d'identification de votre projet et votre agent de codage AI.

   Vous allez saisir un nom de profil pour votre projet. Ce nom de profil indique comment votre outil de codage IA accède à vos ressources.

Use your terminal

Exécutez la commande suivante pour télécharger et suivez les instructions de configuration :

```
curl -fsSL https://github.com/aws/agent-toolkit-for-aws/blob/main/setup-
instructions/setup.md
```

Lorsque vous utilisez notre nouvelle AWS expérience, votre agent installe le serveur AWS MCP et vous avez accès à des compétences d'agent qui peuvent être utilisées dans le cadre de vos projets. Vous obtiendrez également un fichier de règles contenant des instructions adaptées à cette expérience. Le fichier de règles vous permettra également de définir le niveau d'aide que vous souhaitez que l'agent fournisse. Les niveaux d'aide pris en charge sont les suivants :

- Faible : pendant que vous construisez, la compétence ne signalera que les risques de sécurité. Il ne proposera aucune amélioration ou alternative à votre architecture.
- Moyen : pendant que vous développez, la compétence peut poser des questions de clarification si elle détecte des problèmes potentiels. Il ne proposera aucune amélioration ou alternative à votre architecture.
- Élevé : pendant que vous construisez, la compétence vous fournira un niveau de soutien élevé. Il proposera des améliorations ou des alternatives à votre architecture.

Travaillez sur plusieurs projets

Chaque projet possède son propre ensemble d'informations d'identification que les outils de codage IA peuvent utiliser pour créer et gérer AWS des ressources en votre nom. Vous utilisez des profils pour accéder à chaque projet. Un profil est un fichier de paramètres de configuration et d'informations d'identification géré par le AWS CLI, et vous attribuez un nom unique à chaque profil.

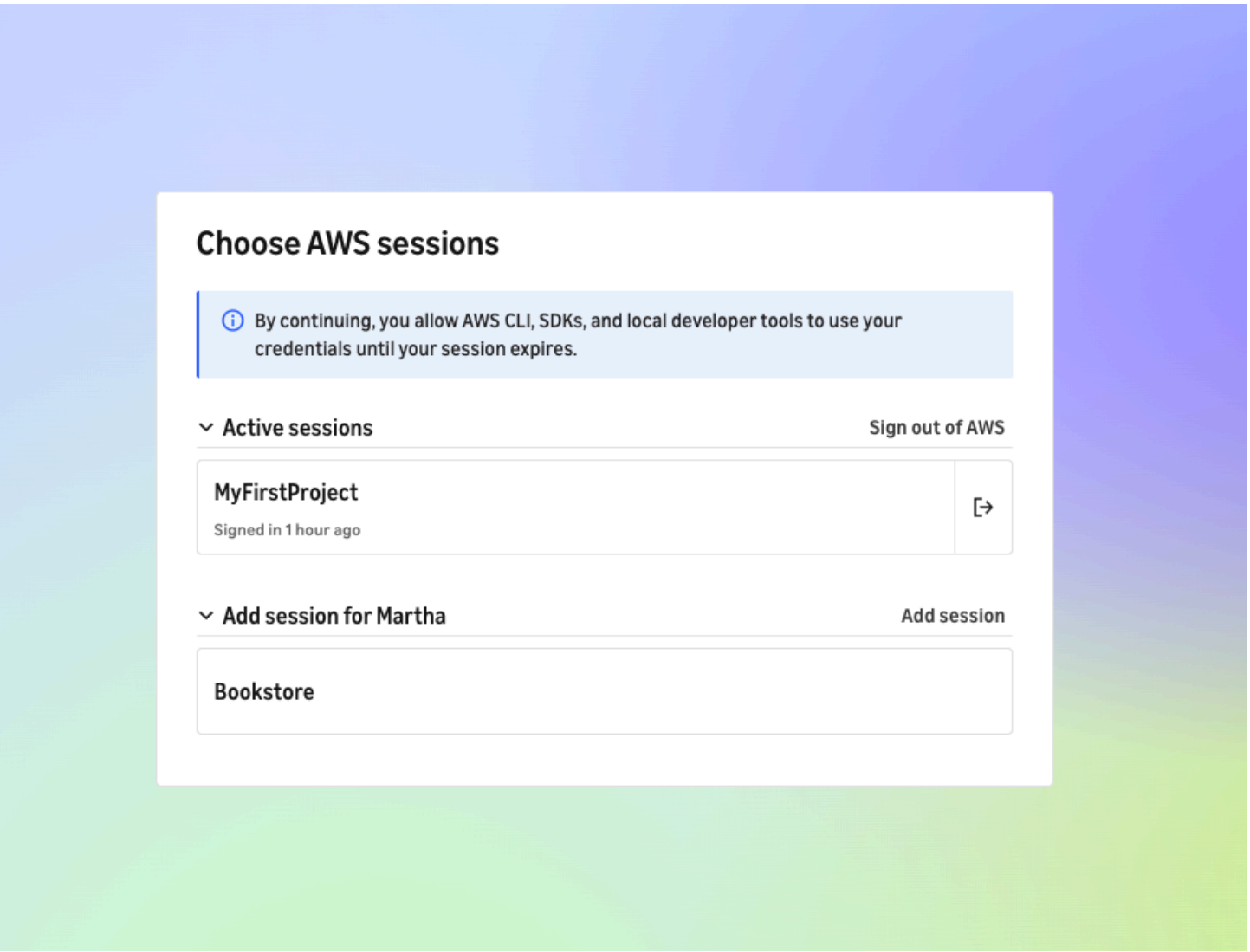
Par exemple, si votre premier projet était `MyFirstProject` et que vous avez choisi le nom du profil `MyFirstProjectProfile` lors de la configuration, vous pouvez accéder à ce projet en vous connectant à l' AWS CLI aide de la commande suivante :

```
aws login --profile MyFirstProjectProfile
```

Si vous créez un autre projet nomméBookstore, vous pouvez y accéder en utilisant le script de configuration et en créant le profilBookstoreProfile. Vous pouvez ensuite vous connecter à l' AWS CLI aide de la commande suivante :

```
aws login --profile BookstoreProfile
```

Toutefois, lorsque vous exécutez l'une de ces commandes, vous devez choisir une session pour vos AWS informations d'identification sur la page Choisir les AWS sessions.



Cette page indique les sessions actives et les sessions que vous pouvez ajouter. Une session représente votre état authentifié à l'aide de vos AWS informations d'identification et fournit les mêmes informations d'identification que celles utilisées par votre agent de codage IA pour créer et gérer des ressources.

Dans cet exemple, vous êtes déjà connecté `MyFirstProject` et vous ne l'êtes pas encore`Bookstore`. Sur la page Choisir AWS les sessions, vous pouvez effectuer les opérations suivantes :

- Pour continuer à utiliser AWS for`MyFirstProject`, choisissez`MyFirstProject`.
- Pour y accéder`Bookstore`, choisissez`Bookstore`.

- Pour supprimer l'une des sessions en cours, cliquez sur l'icône de sortie.
- Pour accéder et Compte AWS utiliser un utilisateur IAM, tel qu'un compte que vous avez créé avecInscrivez-vous pour AWS (avancé), choisissez Ajouter une session.

Les informations d'identification que vous choisirez seront les mêmes que celles que votre agent de codage IA utilise pour créer et gérer des ressources. Par exemple, vous pouvez vous connecter à l' AWS CLI aide de la commande suivante :

```
aws login --profile MyFirstProjectProfile
```

Si vous choisissez ensuite la `Bookstore` session, votre outil de codage IA créera AWS des ressources dans le `Bookstore` projet.

Choisissez toujours la session qui correspond au projet associé à votre profil.

AWS actions pour les porteurs de projets

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Lorsque vous êtes propriétaire de votre projet, vous en avez le contrôle administratif. Cela inclut les tâches que vous pouvez effectuerUtilisation AWS Settings. Il est également possible d'effectuer des actions root uniquement. Ces actions ne peuvent pas être effectuées par les membres de votre équipe.

Les actions que vous pouvez actuellement effectuer uniquement en mode root sont les suivantes :

- Modifiez ou supprimez une politique de compartiment S3 qui refuse tous les principaux. Vous pouvez procéder ainsi pour déverrouiller un compartiment S3 dont la politique de compartiment est mal configurée.
- Modifiez ou supprimez une politique basée sur les ressources SQS qui refuse tous les principaux. Vous pouvez procéder ainsi pour déverrouiller une file d'attente SQS dont la politique basée sur les ressources est mal configurée.

Pour effectuer une action en mode root uniquement

1. Connectez-vous à votre projet et ouvrez la console IAM à https://console.aws.amazon.com/iam/ l'adresse.
2. Dans le volet de navigation de la console, choisissez Gestion de l'accès racine.
3. Pour l'action privilégiée, choisissez l'action privilégiée que vous souhaitez effectuer sur le compte du membre.
   - Sélectionnez Supprimer la politique de compartiment Amazon S3 pour supprimer une politique de compartiment mal configurée qui empêche tous les principaux d'accéder au compartiment Amazon S3.
     a. Entrez l'URI S3 ou choisissez Parcourir S3 pour sélectionner un nom parmi les compartiments de votre projet.
     b. Choisissez Supprimer la politique de compartiment.
     c. Utilisez la console Amazon S3 pour corriger la politique de compartiment après avoir supprimé la politique mal configurée. Pour plus d'informations, consultez Ajout d'une politique de compartiment à l'aide de la console Amazon S3 dans le Guide de l'utilisateur Amazon S3.
   - Sélectionnez Supprimer la politique Amazon SQS pour supprimer une politique basée sur les ressources qui empêche tous les principaux d'accéder à une file d'attente Amazon SQS.
     a. Entrez le nom de la file dans le champ Nom de la file d'attente SQS.
     b. Choisissez Supprimer la politique SQS.
     c. Utilisez la console Amazon SQS pour corriger la politique de la file d'attente après avoir supprimé la politique mal configurée. Pour plus d'informations, consultez Configuration de stratégie d'accès dans Amazon SQS dans le Guide du développeur Amazon SQS.

Mettez à jour votre mot de passe dans AWS Settings

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Vous pouvez mettre à jour votre mot de passe dans AWS les paramètres.

Pour mettre à jour votre mot de passe dans AWS Settings

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Gérer la sécurité et vous connecter.

   Vous serez redirigé vers votre profil AWS Builder ID.
3. Pour Autorisation, choisissez Mettre à jour le mot de passe.
4. Dans le champ Current password (Mot de passe actuel), saisissez le mot de passe que vous utilisez actuellement.
5. Pour Nouveau mot de passe, entrez un nouveau mot de passe.

   AWS exige 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 ! @ # $ % ^ & * () <> [] {} | _ + - =
6. Pour Confirmer le nouveau mot de passe, entrez votre nouveau mot de passe.
7. Choisissez Mettre à jour.

Gérez l'authentification multifactorielle (MFA) dans AWS Settings

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Multi-factor l'authentification (MFA) est un mécanisme simple et efficace pour renforcer votre sécurité. Le premier facteur, votre mot de passe, est un secret que vous mémorisez, également appelé facteur de connaissance. Les autres facteurs peuvent être des facteurs liés à la possession (quelque chose que vous possédez, comme une clé de sécurité) ou des facteurs inhérents (quelque chose que vous êtes, comme un scan biométrique). Nous vous recommandons vivement de configurer le MFA pour ajouter une couche supplémentaire à votre compte.

Vous pouvez enregistrer un authentificateur intégré et également enregistrer une clé de sécurité que vous conservez dans un endroit physiquement sécurisé. Si vous ne parvenez pas à utiliser

votre authentificateur intégré, vous pouvez utiliser votre clé de sécurité enregistrée. Pour les applications d'authentification, vous pouvez également activer la fonctionnalité de sauvegarde ou de synchronisation dans le cloud dans ces applications. Cela vous permet d'éviter de perdre l'accès à votre profil si vous perdez ou cassez votre appareil MFA.

Points clés

Gardez les points essentiels suivants à l'esprit lorsque vous enregistrez et gérez des appareils MFA :

- Nous vous recommandons d'enregistrer plusieurs appareils MFA. Si vous perdez l'accès à tous les appareils MFA enregistrés, vous ne pourrez pas récupérer votre compte.
- Nous vous recommandons de vérifier régulièrement les dispositifs MFA enregistrés pour vous assurer qu'ils sont à jour et fonctionnels. En outre, vous devez stocker ces appareils dans un endroit physiquement sûr lorsqu'ils ne sont pas utilisés.
- Si vous avez créé votre compte à l'aide de Continue with Google, vous pouvez activer l'authentification multifactorielle via votre compte Google. Pour plus de détails, voir Activer la validation en deux étapes.
- Si vous avez créé votre compte à l'aide de Continuer avec Apple, l'authentification multifactorielle est probablement déjà activée dans votre compte Apple. Si ce n'est pas le cas, pour savoir comment l'activer, consultez la section Two-factor Authentification pour le compte Apple.
- Si vous avez créé votre compte à l'aide de Continuer avec GitHub, vous pouvez activer l'authentification multifactorielle via votre GitHub compte. Pour plus de détails, consultez Configuration (GitHub) de l'authentification à deux facteurs.
- Si vous avez créé votre compte à l'aide de Continue with Amazon, vous pouvez activer l'authentification multifactorielle via votre compte Amazon. Pour plus de détails, voir Qu'est-ce que la Two-Step vérification ? .

Types de MFA disponibles pour notre nouveau AWS expérience

Notre nouvelle AWS expérience prend en charge les types d'appareils d'authentification multifactorielle (MFA) suivants.

Authentificateurs FIDO2

FIDO2 est une norme qui inclut le CTAP2 WebAuthnet qui est basée sur la cryptographie à clé publique. Les informations d'identification FIDO résistent au hameçonnage car elles sont uniques au site Web sur lequel elles ont été créées, par exemple. AWS

AWS prend en charge les deux formats les plus courants pour les authentificateurs FIDO : les authentificateurs intégrés et les clés de sécurité. Voir ci-dessous pour plus d'informations sur les types les plus courants d'authentificateurs FIDO.

Built-in authentificateurs

Certains appareils sont dotés d'authentificateurs intégrés, tels que TouchID activé MacBook ou un appareil photo Windows. Hello-compatible Si votre appareil est compatible avec les protocoles FIDO, notamment WebAuthn, vous pouvez utiliser votre empreinte digitale ou votre visage comme deuxième facteur. Pour plus d'informations, consultez la section Authentification FIDO.

Clés de sécurité

Vous pouvez acheter une clé USB, BLE ou NFC-connected de sécurité FIDO2-compatible externe. Lorsque vous êtes invité à entrer un appareil MFA, appuyez sur le capteur de la touche. YubiKey ou Feitian fabrique des appareils compatibles. Pour une liste de toutes les clés de sécurité compatibles, consultez la section Produits certifiés FIDO.

Gestionnaires de mots de passe, fournisseurs de clés d'accès et autres authentificateurs FIDO

Plusieurs fournisseurs tiers prennent en charge l'authentification FIDO dans les applications mobiles, en tant que fonctionnalité dans les gestionnaires de mots de passe, les cartes à puce dotées d'un mode FIDO et d'autres formats. Ces FIDO-compatible appareils peuvent fonctionner avec IAM Identity Center, mais nous vous recommandons de tester vous-même un authentificateur FIDO avant d'activer cette option pour le MFA.

> **Note**
>
> Certains authentificateurs FIDO peuvent créer des informations d'identification FIDO détectables appelées clés d'accès. Les clés d'accès peuvent être liées à l'appareil qui les a créées, ou elles peuvent être synchronisées et sauvegardées dans un cloud. Par exemple, vous pouvez enregistrer une clé d'accès à l'aide d'Apple Touch ID sur un Macbook compatible, puis vous connecter à un site depuis un ordinateur portable Windows à l'aide de Google Chrome avec votre clé d'accès dans iCloud en suivant les instructions qui s'affichent à l'écran lors de la connexion. Pour plus d'informations sur les appareils compatibles avec les clés d'accès synchronisées et sur l'interopérabilité actuelle des clés d'accès entre les systèmes d'exploitation et les navigateurs, consultez la section Support des appareils sur passkeys.dev, une ressource gérée par l'Alliance FIDO et le World Wide Web Consortium (W3C).

Applications d'authentification

Les applications d'authentification sont des authentificateurs tiers basés sur un mot de passe à usage unique (OTP). Vous pouvez utiliser une application d'authentification installée sur votre appareil mobile ou votre tablette en tant qu'appareil MFA autorisé. L'application d'authentification tierce doit être conforme à la RFC 6238, qui est un algorithme de mot de passe à usage unique (TOTP) basé sur des normes et basé sur le temps capable de générer des codes d'authentification à six chiffres.

Lorsque vous êtes invité à saisir le MFA, vous devez saisir un code valide provenant de votre application d'authentification dans la zone de saisie qui s'affiche. Chaque dispositif MFA attribué à un utilisateur doit être unique. Deux applications d'authentification peuvent être enregistrées pour un utilisateur donné.

Vous pouvez choisir parmi les applications d'authentification tierces bien connues suivantes. Cependant, toutes les TOTP-compliant applications fonctionnent avec AWS Builder ID MFA.

Système d'exploitation	Application d'authentification testée
Android	1Password, Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator
iOS	1Password, Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator

Enregistrez votre appareil MFA

> **Note**
>
> Une fois que vous vous êtes inscrit à l'authentification MFA, que vous vous êtes déconnecté, puis que vous vous êtes connecté sur le même appareil, il se peut que vous ne soyez pas invité à utiliser l'authentification MFA sur les appareils approuvés.

Pour enregistrer votre appareil MFA à l'aide d'une application d'authentification

1. Ouvrez AWS les paramètres sur https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Gérer la sécurité et la connexion.

Vous serez redirigé vers votre profil AWS Builder ID.

3. Sur la page Sécurité, choisissez Enregistrer l'appareil.
4. Sur la page Enregistrer un appareil MFA, choisissez l'application Authenticator.
5. AWS Builder ID fonctionne et affiche les informations de configuration, y compris un graphique de code QR. Le graphique est une représentation de la « clé de configuration secrète » qui peut être saisie manuellement dans les applications d'authentification qui ne prennent pas en charge les codes QR.
6. Ouvrez votre application d'authentification. Pour obtenir la liste des applications, consultezApplications d'authentification.

   Si l'application d'authentification prend en charge plusieurs appareils ou comptes MFA, choisissez l'option permettant de créer un nouvel appareil ou un nouveau compte MFA.
7. Déterminez si l'application MFA prend en charge les codes QR, puis effectuez l'une des opérations suivantes sur la page Configurer votre application d'authentification :

   1. Choisissez Afficher le code QR, puis utilisez l'application pour scanner le code QR. Par exemple, vous pouvez choisir l'icône de l'appareil photo ou une option similaire à Scanner le code. Utilisez ensuite l'appareil photo de l'appareil pour scanner le code.
   2. Choisissez Afficher la clé secrète, puis entrez cette clé secrète dans votre application MFA.

   Lorsque vous aurez terminé, votre application d'authentification générera et affichera un mot de passe à usage unique.
8. Dans le champ Code d'authentification, entrez le mot de passe à usage unique qui apparaît actuellement dans votre application d'authentification. Choisissez Assign MFA (Affecter le MFA).

> **Important**
>
> Envoyez votre demande immédiatement après avoir généré le code. Si vous générez le code puis attendez trop longtemps pour envoyer la demande, le dispositif MFA est correctement associé à votre AWS Builder ID, mais le dispositif MFA n'est pas synchronisé. En effet, les TOTP (Time-based One-Time Passwords ou mots de passe à usage unique à durée limitée) expirent après une courte période. Dans ce cas, vous pouvez resynchroniser le dispositif. Pour plus d'informations, consultez *I get the*

```
    message 'An unexpected error has occurred' when I try to register
    or sign in with an authenticator app.
```

9. Pour attribuer un nom convivial à votre appareil dans AWS Builder ID, choisissez Renommer. Ce nom vous permet de distinguer cet appareil des autres appareils que vous enregistrez.

Le dispositif MFA est désormais prêt à être utilisé avec les AWS paramètres, vos projets et le AWS Builder ID.

Enregistrez une clé de sécurité en tant que dispositif MFA

Pour enregistrer votre appareil MFA à l'aide d'une clé de sécurité

1. Ouvrez AWS les paramètres sur https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Gérer la sécurité et la connexion.

   Vous serez redirigé vers votre profil AWS Builder ID.
3. Sur la page Sécurité, choisissez Enregistrer l'appareil.
4. Sur la page Enregistrer un appareil MFA, sélectionnez Clé de sécurité.
5. Assurez-vous que votre clé de sécurité est activée. Si vous utilisez une clé de sécurité physique distincte, connectez-la à votre ordinateur.
6. Suivez les instructions qui s'affichent à l'écran. Votre expérience varie en fonction de votre système d'exploitation et de votre navigateur.
7. Pour attribuer un nom convivial à votre appareil dans AWS Builder ID, choisissez Renommer. Ce nom vous permet de distinguer cet appareil des autres appareils que vous enregistrez.

Le dispositif MFA est désormais prêt à être utilisé avec les AWS paramètres, vos projets et le AWS Builder ID.

Renommez votre appareil MFA

Pour renommer votre appareil MFA

1. Ouvrez AWS les paramètres sur https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Gérer la sécurité et la connexion.

   Vous serez redirigé vers votre profil AWS Builder ID.

3. Choisissez Security (Sécurité). Lorsque vous arrivez sur la page, vous voyez que Renommer est grisé.
4. Sélectionnez le périphérique MFA que vous souhaitez modifier. Cela vous permet de choisir Renommer. Ensuite, une boîte de dialogue apparaît.
5. Dans l'invite qui s'affiche, entrez le nouveau nom dans le champ Nom du périphérique MFA, puis choisissez Renommer. L'appareil renommé apparaît sous Multi-factor Appareils d'authentification (MFA).

Supprimer votre appareil MFA

Nous vous recommandons de conserver au moins deux appareils MFA actifs. Pour désactiver l'authentification multifactorielle, supprimez tous les appareils MFA enregistrés de votre profil.

Pour supprimer un appareil MFA

1. Ouvrez AWS les paramètres sur https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Gérer la sécurité et la connexion.

   Vous serez redirigé vers votre profil AWS Builder ID.
3. Sur la page Sécurité, sélectionnez le périphérique MFA que vous souhaitez modifier et choisissez Supprimer.
4. Dans le dispositif Delete MFA ? modal, suivez les instructions pour supprimer votre appareil.
5. Sélectionnez Supprimer.

L'appareil supprimé n'apparaît plus sous les appareils Multi-factor d'authentification (MFA).

Supprimer toutes les sessions dans AWS Settings

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Vous pouvez supprimer toutes les sessions sur tous les appareils dans AWS les paramètres. Si vous ne reconnaissez pas un appareil, modifiez votre mot de passe et supprimez toutes les sessions.

Pour supprimer toutes les sessions

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Gérer la sécurité et vous connecter.

   Vous serez redirigé vers votre profil AWS Builder ID.
3. Pour les appareils connectés, choisissez Supprimer toutes les sessions.
4. Confirmez votre choix et choisissez Supprimer toutes les sessions.

Vous serez déconnecté des AWS paramètres.

Gérez votre nom ou votre surnom dans AWS Settings

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Vous pouvez modifier votre nom à tout moment. Tous les membres de l'équipe peuvent voir votre nom, et si vous êtes passé au forfait payant, c'est le nom qui apparaît sur vos informations de facturation. Si vous vous êtes inscrit AWS en Inde, votre nom doit correspondre exactement au nom qui apparaît sur le document que vous comptez utiliser pour la vérification client.

Lorsque vous modifiez votre nom, vous modifiez le nom dans votre AWS Builder ID. Cela aura un impact sur votre nom dans AWS les paramètres, sur AWS Builder ID et sur toutes AWS les ressources auxquelles vous accédez directement via le AWS Builder ID.

Votre nom est la façon dont vous êtes désigné dans les outils et les services lorsque vous interagissez avec les autres. Votre surnom indique la manière dont vous souhaitez être connu AWS, vos amis et les autres personnes avec lesquelles vous collaborez étroitement.

Pour modifier votre nom ou votre surnom

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Gérer le profil.
3. Pour les informations de profil, choisissez Gérer le profil.

Vous serez redirigé vers votre profil AWS Builder ID.

4. Pour les informations de profil, choisissez Modifier.
5. (Facultatif) Dans Nom, entrez un nouveau nom.
6. (Facultatif) Dans le champ Surnom, entrez un nouveau surnom.
7. Sélectionnez Enregistrer les modifications.

Changez votre adresse e-mail dans AWS Settings

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Vous pouvez modifier votre adresse e-mail dans AWS les paramètres. Lorsque vous modifiez votre adresse e-mail, votre adresse e-mail précédente sera séparée de votre AWS profil et de votre identifiant AWS Builder. Vous ne pourrez pas utiliser cet e-mail pour accéder aux projets dans AWS les paramètres, mais vous pouvez utiliser cet e-mail pour vous AWS réinscrire.

Votre adresse e-mail est partagée avec les membres de l'équipe lorsque vous leur donnez accès à vos projets.

Pour modifier votre adresse e-mail

1. Ouvrez AWS les paramètres sur https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Gérer le profil.
3. Pour les informations sur le profil, choisissez Gérer le profil.

   Vous serez redirigé vers votre profil AWS Builder ID.
4. Pour les informations de contact, choisissez Modifier.
5. Pour Adresse e-mail, entrez une nouvelle adresse e-mail et choisissez Vérifier l'e-mail. Nous vous enverrons un code de vérification pour votre nouvelle adresse e-mail. Vous le saisirez dans la fenêtre contextuelle Vérifier l'e-mail.
6. Pour le code de vérification, entrez le code de vérification que nous avons envoyé à votre nouvel e-mail.

7. Choisissez Vérifier.

Modifiez vos informations de contact dans AWS Settings

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Vous pouvez modifier votre numéro de téléphone ou l'adresse associée aux AWS paramètres. Lorsque vous modifiez ces valeurs, elles peuvent avoir un impact sur les obligations fiscales.

Pour modifier vos informations de contact

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Gérer le profil.
3. Pour les informations de contact, choisissez Modifier.
4. Entrez de nouvelles informations de contact.
5. Choisissez Enregistrer.

Désactivez l'utilisation de votre contenu pour améliorer le service dans AWS Settings

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

AWS Les services d'IA peuvent utiliser et stocker le contenu des clients pour améliorer le service, par exemple pour résoudre des problèmes opérationnels, évaluer les performances du service, déboguer ou former des modèles. À cette fin, nous pouvons stocker ce contenu en Région AWS dehors de l' Région AWS endroit où vous utilisez le service. Vous pouvez refuser l'utilisation de votre contenu à des fins d'amélioration du service via AWS les paramètres. La désinscription a pour effet

d'associer une politique AWS de désinscription aux services d'IA à votre AWS organisation. Pour plus d'informations sur les politiques de désinscription, consultez la documentation sur les politiques de désinscription des services d'IA.

En choisissant de vous désinscrire de tous les services, vous retirerez tous vos projets des améliorations de service utilisant votre contenu pour les services d'IA pris en charge actuels et futurs, soutenus par les politiques de désinscription des services d'IA.

Des étapes supplémentaires sont nécessaires pour vous désinscrire d'Amazon Monitron. Pour plus d'informations, consultez Conditions de service AWS. Seul le propriétaire du projet peut refuser l'utilisation des données par les services d' AWS IA.

Pour refuser l'utilisation des données par AWS Services d'IA

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Project.
3. Pour la vue d'ensemble, choisissez Actions, puis choisissez Désactiver l'utilisation des données par les services d' AWS IA.
4. Confirmez votre choix et choisissez Se désinscrire.

Demandez votre AWS Données d'identification du constructeur

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Vous pouvez demander et consulter les informations personnelles associées à votre AWS Builder ID et aux AWS applications et services auxquels vous avez accédé avec votre AWS Builder ID. Nous traiterons votre demande dans les 30 jours et vous informerons lorsque vos données seront prêtes. Tant que votre demande de données est en attente, vous ne pouvez pas fermer votre AWS profil. Vous pouvez toujours fermer des projets ou fermer l'organisation propriétaire de tous vos projets.

Pour plus d'informations sur l'exercice de vos droits en tant que personne concernée, y compris pour les informations personnelles fournies en relation avec d'autres AWS sites Web, applications, produits, services, événements et expériences, consultez la section AWS Confidentialité.

Pour demander vos données

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Gérer le profil.
3. Choisissez Gérer le profil.

   Vous serez redirigé vers votre profil AWS Builder ID.
4. Choisissez Confidentialité et données.
5. Choisissez de demander vos données Builder ID ou vos AWS données.

   Un message de confirmation vert apparaît en haut de la page indiquant que nous avons reçu votre demande et celle-ci sera traitée dans les 30 jours.
6. Lorsque vous recevez un e-mail de notre part indiquant que la demande a été traitée, revenez à la page Confidentialité et données de votre profil AWS Builder ID. Cliquez sur le nouveau bouton disponible Télécharger l'archive ZIP avec vos données.

Tant que votre demande de données est en attente, vous ne pourrez pas supprimer votre AWS Builder ID.

Créez un projet dans AWS Settings

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Un projet contient un single Compte AWS dans lequel vous créez des AWS ressources. Un projet inclut également des paramètres de partage avec d'autres collaborateurs. Les AWS ressources que vous créez doivent représenter une application ou un ensemble de cas d'utilisation connexes. Un projet peut couvrir les environnements de développement et de production de votre application. Par exemple, vous pouvez créer un projet appelé Bookstore qui contient des ressources pour une application de librairie, notamment une base de données, des ressources informatiques et du stockage.

Vous pouvez partager ce projet avec d'autres membres de l'équipe, qui peuvent créer et gérer des ressources pour l'application de librairie.

Chaque projet possède ses propres contrôles des coûts basés sur les ressources du compte. Si vous utilisez le forfait payant, vous pouvez configurer une limite de dépenses dans AWS les paramètres pour chaque projet. Pour plus d’informations, consultez Créez une limite de dépenses dans AWS Settings. En tant que propriétaire du projet, vous êtes responsable des factures mensuelles pour les frais d'utilisation et les frais récurrents.

Considérations relatives à la création d'un projet

- Vous pouvez accéder à des projets dont vous n'êtes pas propriétaire en tant que membre de l'équipe.
- Le nom de chaque projet doit être propre à vos projets. Les projets appartenant à d'autres membres de l'équipe peuvent porter le même nom.
- Les noms de projets peuvent contenir les caractères valides suivants : a-z A-Z, 0-9 et points (.).
- Lorsque vous créez votre projet, AWS attribuez-le à une région (USA Est (Ohio) (`us-east-2`), Europe (Stockholm) () ou Asie-Pacifique (Sydney`eu-north-1`) (`ap-southeast-2`), en fonction du pays indiqué dans votre adresse de contact (États-Unis d'Amérique, Europe ou Asie-Pacifique). Toutes les ressources régionales que vous créez seront hébergées dans cette région. Pour plus d’informations, consultez Régions AWS pour vos projets.

Pour créer un projet

Pour créer un projet

1. Ouvrez AWS les paramètres sur https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Project.
3. Sélectionnez Create a project (Créer un projet).
4. Dans Nom du projet, entrez un nom descriptif pour votre projet.

   Ce nom est communiqué aux membres de l'équipe lorsque vous les invitez à collaborer.
5. Cliquez sur Créer.

La création de votre projet ne prend que quelques secondes. Lorsque votre projet est disponible, vous pouvez le choisir et accéder au Console de gestion AWS pour commencer à le construire.

Si vous avez déjà configuré votre outil de codage AI pour qu'il interagisse avec votre Compte AWS, vous pouvez lui demander de créer des ressources dans votre nouveau projet.

Utilisez les exemples d'instructions de votre outil de codage AI pour commencer :

```
What is the Region for my project test project?
```

```
Create a hello world Lambda function in my project test project.
```

```
Create an S3 bucket in my project test project.
```

Régions AWS pour vos projets

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Lorsque vous créez votre projet, AWS attribuez-le à une région (États-Unis Est (Ohio) (`us-east-2`), Europe (Stockholm) (`eu-north-1`) ou Asie-Pacifique (Sydney) (`ap-southeast-2`), en fonction du pays indiqué dans votre adresse de contact (États-Unis, Europe ou Asie-Pacifique). Toutes les ressources régionales que vous créez seront hébergées dans cette région.

Les éléments suivants sont à prendre en compte pour les éléments sélectionnés Région AWS pour votre compte :

- Si vous modifiez vos informations de contact dans AWS les paramètres, la région que vous avez sélectionnée ne changera pas. Si vous devez accéder à une région spécifique, utilisez S'inscrire pour AWS (avancé). Vous pouvez également activer les fonctionnalités avancées de votre compte afin de sélectionner différentes régions.
- AWS peut introduire des régions prises en charge supplémentaires, mais celles-ci ne seront disponibles que pour les nouvelles inscriptions. Pour voir les dernières régions prises en charge au 18 août 2026, consultez les tableaux ci-dessous. Si vous avez déjà un projet, vous pouvez trouver la région que vous avez sélectionnée dans AWS les paramètres.
- Des services mondiaux sont disponibles pour votre projet. Ces services sont accessibles via une seule région qui peut être différente de votre région d'origine. Pour plus d'informations, consultez la section Limites d'isolation des AWS défauts. En outre, certains services sont disponibles dans des régions spécifiques. Dans le Console de gestion AWS, vous pouvez consulter ces services

dans certaines régions, mais vous reviendrez à la région que vous avez sélectionnée lorsque vous naviguerez vers un autre service.

- Si vous utilisez Amazon Bedrock, vous pouvez utiliser des API qui ne créent pas de ressources dans toutes les publicités et Régions AWS qui sont activées par défaut.
- Si vous l'utilisez CloudFront, certaines fonctionnalités qui créeraient des ressources en dehors de la région que vous avez sélectionnée ne sont pas disponibles. Cela inclut l'utilisation AWS WAF avec CloudFront.
- Certains CloudTrail événements impliquant les services mondiaux sont enregistrés dans la région où le service mondial opère. Vous avez accès à ces événements.
- AWS WAF et Amazon CloudWatch Logs sont disponibles dans l'est des États-Unis (Virginie du Nord) (`us-east-1`).

Vous pouvez trouver la région sélectionnée pour tous les projets de votre compte en utilisant AWS les paramètres. Dans le Console de gestion AWS, la plupart des consoles de service sont hébergées dans la région dans laquelle vous vous trouvez, y compris Bedrock et SageMaker. Si vous consultez une console de service depuis un service mondial, la console achemine automatiquement tous vos appels d'API vers la région appropriée pour le service mondial.

Trouvez la sélection Région AWS pour vos projets

À titre de meilleure pratique, nous vous recommandons de toujours confirmer les Région AWS informations pour votre projet avant de créer des AWS ressources.

Pour trouver la sélection Région AWS pour vos projets

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Project.
3. Dans la section Vue d'ensemble, choisissez Informations supplémentaires.

   Dans cette vue, vous pouvez également trouver l' Compte AWS ID associé à votre projet.
4. Pour la région, vous verrez que Région AWS votre projet a été provisionné.

Lorsque vous créez AWS des ressources régionales dans l'un de vos projets, les noms des ressources Amazon de ces ressources l'incluent Région AWS.

Pays où des ressources régionales sont approvisionnées dans l'est des États-Unis (Ohio) (us-east-2)

Nom du pays	Code pays
Antigua et Barbuda	AG
Argentine	AR
Bahamas	BS
Barbade	BB
Belize	BZ
Bolivie	BO
Brésil	BR
Canada	CA
Chili	CL
Colombie	CO
Costa Rica	CR
Dominique	DM
République Dominicaine	DO
Equateur	EC
El Salvador	SV
Grenade	GD
Guatemala	GT
Guyane	GY

Nom du pays	Code pays
Haïti	HT
Honduras	HN
Jamaïque	JM
Mexique	MX
Nicaragua	NI
Panama	PA
Paraguay	PY
Pérou	PE
Saint Kitts et Nevis	KN
Sainte-Lucie	LC
Saint-Vincent-et-les-Grenadines	VC
Suriname	SR
Trinidad et Tobago	TT
États-Unis	ETATS-UNIS
Uruguay	UY
Venezuela	VE
Anguilla	AI
Aruba	AW
Bermudes	BM
Bonaire, Saint-Eustache et Saba	BQ

Nom du pays	Code pays
Îles Vierges Britanniques	VG
Iles Caïmans	KY
Curaçao	CW
Îles Malouines	FK
Guyane française	GF
Guadeloupe	GP
Martinique	MQ
Montserrat	MS
Porto Rico	PR
Saint-Barthélemy	BL
Saint-Martin	MF
Saint-Pierre-et-Miquelon	PM
Sint Maarten	SX
Iles Turks et Caicos	TC
U.S. Îles Vierges	VI

Pays où des ressources régionales sont fournies en Asie-Pacifique (Sydney) (ap-southeast-2)

Nom du pays	Code pays
Afghanistan	AF

Nom du pays	Code pays
Australie	AU
Bangladesh	BD
Bhoutan	BT
Brunei	BN
Cambodge	KH
Chine	CN
Timor oriental () Timor-Leste	TL
Fidji	FJ
Hong Kong	HK
Inde	IN
Indonésie	ID
Japon	JP
Kazakhstan	KZ
Kiribati	KI
Kirghizstan	KG
Laos	LA
Macao	MO
Malaisie	MY
Maldives	MV
Îles Marshall	MH

Nom du pays	Code pays
Micronésie	FM
Mongolie	MN
Birmanie	MM
Nauru	NR
Népal	NP
Nouvelle-Zélande	NZ
Pakistan	PK
Palaos	PW
Papouasie-Nouvelle-Guinée	PG
Philippines	PH
Samoa	WS
Singapour	SG
Iles Salomon	SB
Corée du Sud	KR
Sri Lanka	LK
Taïwan	TW
Tadjikistan	TJ
Thaïlande	TH
Tonga	TO
Turkménistan	TM

Nom du pays	Code pays
Tuvalu	TV
Ouzbékistan	UZ
Vanuatu	VU
Vietnam	VN
Samoa américaines	AS
Île Christmas	CX
Îles Cocos (Keeling)	CC
Iles Cook	CK
Polynésie française	PF
Guam	GU
Île et McDonald îles Heard	HM
Nouvelle-Calédonie	NC
Niué	NU
Île Norfolk	NF
Îles Mariannes du Nord	MP
Îles Pitcairn	PN
Tokélaou	TK
U.S. Îles mineures éloignées	UM
Wallis et Futuna	WF

Pays où des ressources régionales sont fournies en Europe (Stockholm) (eu-north-1)

Nom du pays	Code pays
Albanie	AL
Algérie	DZ
Andorre	AD
Angola	AO
Arménie	AM
Autriche	À
Azerbaïdjan	AZ
Bahreïn	BH
Biélorussie	BY
Belgique	BE
Bénin	BJ
Bosnie-Herzégovine	BA
Botswana	BW
Bulgarie	BG
Burkina Faso	BF
Burundi	BI
Cap-Vert	CV
Cameroun	CM

Nom du pays	Code pays
République centrafricaine	CF
Tchad	TD
Comores	KM
Congo (Brazzaville)	CG
Congo (RDC)	CD
Côte d'Ivoire	CI
Croatie	HR
Chypre	CY
République tchèque	CZ
Danemark	DK
Djibouti	DJ
Egypte	EG
Guinée équatoriale	GQ
Érythrée	ER
Estonie	EE
Eswatini	SZ
Ethiopie	ET
Finlande	FI
France	FR
Gabon	GA

Nom du pays	Code pays
Gambie	GM
Géorgie	GE
Allemagne	DE
Ghana	GH
Grèce	GR
Guinée	GN
Guinea-Bissau	GW
Hongrie	HU
Islande	IS
Irak	IQ
Irlande	IE
Israël	IL
Italie	IT
Jordanie	JO
Kenya	KE
Kosovo	XK
Koweït	KW
Lettonie	LV
Liban	LB
Lesotho	LS

Nom du pays	Code pays
Liberia	LR
Libye	LY
Liechtenstein	LI
Lituanie	LT
Luxembourg	LU
Madagascar	MG
Malawi	MW
Mali	ML
Malte	MT
Mauritanie	MR
Maurice	MU
Moldavie	MD
Monaco	MC
Monténégro	ME
Maroc	MA
Mozambique	MZ
Namibie	NA
Pays-Bas	NL
Niger	NE
Nigeria	NG

Nom du pays	Code pays
Macédoine du Nord	MK
Norvège	NO
Oman	OM
Palestine	PS
Pologne	PL
Portugal	PT
Qatar	QA
Roumanie	RO
Russie	RU
Rwanda	RW
Saint-Marin	SM
Sao Tomé-et-Principe	ST
Arabie saoudite	SA
Sénégal	SN
Serbie	RS
Seychelles	SC
Sierra Leone	SL
Slovaquie	SK
Slovénie	SI
Somalie	SO

Nom du pays	Code pays
Afrique du Sud	ZA
Soudan du Sud	SS
Espagne	ES
Suède	SE
Suisse	CH
Tanzanie	TZ
Togo	TG
Tunisie	TN
Turquie	TR
Ouganda	UG
Ukraine	UA
Emirats arabes unis	AE
Royaume-Uni	Go
Cité du Vatican	VA
Yémen	YE
Zambie	ZM
Zimbabwe	ZW
Îles Åland	AX
Antarctique	AQ
Île Bouvet	BV

Nom du pays	Code pays
Territoire Britannique de l'Océan Indien	E/S
Iles Féroé	FO
Terres australes et antarctiques françaises	TF
Gibraltar	GI
Groenland	GL
Guernesey	GG
Île de Man	IM
Jersey	JE
Mayotte	YT
La Réunion	RE
Sainte-Hélène	SH
Géorgie du Sud et îles Sandwich du Sud	GS
Svalbard et Île Jan Mayen	SJ
Sahara occidental	EH

Politiques gérées pour votre organisation

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Lorsque vous utilisez notre nouvelle AWS expérience, AWS gère les politiques de gestion de l'organisation, y compris les politiques de contrôle des ressources (RCP) et les politiques de contrôle

des services (SCP). Ces contrôles de protection empêchent le propriétaire du projet ou un membre de l'équipe d'effectuer des actions qui empêcheraient les paramètres par défaut AWS préconfigurés définis pour vous aider à créer et à développer rapidement.

Politiques de contrôle des services pour les projets

La politique de contrôle des services ci-dessous s'applique à tous les utilisateurs d'un projet et ne peut pas être modifiée :

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BlockOrgEscape",
      "Effect" : "Deny",
      "Action" : [
        "account:CloseAccount",
        "organizations:AcceptHandshake",
        "organizations:LeaveOrganization",
        "sso:CreateInstance"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ProtectManagedRoles",
      "Effect" : "Deny",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:TagRole",
        "iam:UntagRole",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole"
      ],
      "Resource" : "arn:*:iam::*:role/managed/*",
      "Condition" : {
        "StringNotLike" : {
```

```
          "aws:PrincipalArn" : "arn:*:iam::*:role/managed/
AWSManagedAccountManagementAccessRole"
        }
      }
    }
  ]
}
```

Cette politique n'est pas supprimée lorsque vous activez les fonctionnalités avancées. Pour plus d'informations, consultez Activer le mode avancé AWS fonctionnalités.

Une fois que vous avez activé les fonctionnalités avancées, cette politique reste attachée à la racine de votre organisation. Elle s'applique donc à tous les comptes membres, y compris les comptes que vous créez ou invitez ultérieurement.

En outre, nous appliquons la politique de contrôle des services suivante à tous les utilisateurs d'un projet afin de limiter certaines modifications de votre projet qui ne sont pas prises en charge ou qui doivent être effectuées dans AWS les paramètres :

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BlockAccountManagementAPIs",
      "Effect" : "Deny",
      "Action" : [
        "account:AcceptPrimaryEmailUpdate",
        "account:DeleteAlternateContact",
        "account:DisableRegion",
        "account:EnableRegion",
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:GetGovCloudAccountInformation",
        "account:GetRegionOptStatus",
        "account:PutAccountName",
        "account:PutAlternateContact",
        "account:PutContactInformation",
        "account:StartPrimaryEmailUpdate"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyBillingOperations",
```

```
      "Effect" : "Deny",
      "Action" : "billing:*",
      "Resource" : "*"
    },
    {
      "Sid" : "DenyNotificationContactsOperations",
      "Effect" : "Deny",
      "Action" : "notifications-contacts:*",
      "Resource" : "*"
    },
    {
      "Sid" : "DenyRestrictedNotificationOperations",
      "Effect" : "Deny",
      "Action" : [
        "notifications:AssociateChannel",
        "notifications:AssociateManagedNotificationAccountContact",
        "notifications:AssociateManagedNotificationAdditionalChannel",
        "notifications:AssociateOrganizationalUnit",
        "notifications:CreateEventRule",
        "notifications:CreateNotificationConfiguration",
        "notifications:DeleteEventRule",
        "notifications:DeleteNotificationConfiguration",
        "notifications:DeregisterNotificationHub",
        "notifications:DisableNotificationsAccessForOrganization",
        "notifications:DisassociateChannel",
        "notifications:DisassociateManagedNotificationAccountContact",
        "notifications:DisassociateManagedNotificationAdditionalChannel",
        "notifications:DisassociateOrganizationalUnit",
        "notifications:EnableNotificationsAccessForOrganization",
        "notifications:GetEventRule",
        "notifications:GetFeatureOptInStatus",
        "notifications:GetNotificationConfiguration",
        "notifications:GetNotificationEvent",
        "notifications:GetNotificationsAccessForOrganization",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListManagedNotificationChannelAssociations",
        "notifications:ListMemberAccounts",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationEvents",
        "notifications:ListNotificationHubs",
        "notifications:ListOrganizationalUnits",
        "notifications:ListTagsForResource",
        "notifications:PutFeatureOptInStatus",
```

```
        "notifications:RegisterNotificationHub",
        "notifications:TagResource",
        "notifications:UntagResource",
        "notifications:UpdateEventRule",
        "notifications:UpdateNotificationConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyRoleManagerDisablement",
      "Effect" : "Deny",
      "Action" : "iam:PutAccountProperties",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iam:AccountPropertyNamespaces" : "RoleManager"
        }
      }
    }
  ]
}
```

Cette politique est supprimée lorsque vous activez les fonctionnalités avancées. Pour plus d'informations, consultez Activer le mode avancé AWS fonctionnalités.

La suppression de cette règle ne vous permet pas de mettre à jour l'adresse e-mail de l'utilisateur root d'un compte de projet. Pour plus d'informations, consultez Comptes de projet après avoir activé les fonctionnalités avancées.

En outre, nous appliquons également la politique de contrôle des services suivante pour tous les utilisateurs d'un projet, afin de Régions AWS permettre la prise en charge de services partitionnels, en fonction de votre *selected-region* :

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "UsEast1Partitional",
      "Effect" : "Deny",
      "NotAction" : [
        "account:*",
        "acm:*",
        "activate:*",
```

```
        "artifact:*",
        "aws-marketplace:*",
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:CreateInference",
        "bedrock-mantle:GetInference",
        "bedrock-mantle:GetModel",
        "bedrock-mantle:ListModels",
        "bedrock:ApplyGuardrail",
        "bedrock:CountTokens",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:ListFoundationModels",
        "bedrock:ListInferenceProfiles",
        "budgets:*",
        "ce:*",
        "chatbot:*",
        "cloudfront-keyvaluestore:*",
        "cloudfront:*",
        "cloudshell:*",
        "cloudtrail:LookupEvents",
        "cloudwatch:BatchGet*",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "consoleapp:*",
        "cost-optimization-hub:*",
        "ec2:DescribeRegions",
        "ecr-public:*",
        "freetier:*",
        "health:*",
        "iam:*",
        "identitystore-auth:*",
        "identitystore:*",
        "invoicing:*",
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lightsail:AttachCertificateToDistribution",
        "lightsail:CreateCertificate",
```

```
        "lightsail:CreateContactMethod",
        "lightsail:CreateDistribution",
        "lightsail:CreateDomain",
        "lightsail:CreateDomainEntry",
        "lightsail:DeleteAlarm",
        "lightsail:DeleteCertificate",
        "lightsail:DeleteContactMethod",
        "lightsail:DeleteDistribution",
        "lightsail:DeleteDomain",
        "lightsail:DeleteDomainEntry",
        "lightsail:DetachCertificateFromDistribution",
        "lightsail:Get*",
        "lightsail:IsVpcPeered",
        "lightsail:PutAlarm",
        "lightsail:ResetDistributionCache",
        "lightsail:SendContactMethodVerification",
        "lightsail:SetIpAddressType",
        "lightsail:TagResource",
        "lightsail:TestAlarm",
        "lightsail:UntagResource",
        "lightsail:UpdateDistribution",
        "lightsail:UpdateDistributionBundle",
        "lightsail:UpdateDomainEntry",
        "logs:*",
        "managedblockchain-query:*",
        "managedblockchain:*",
        "mapcredits:*",
        "notifications:GetManagedNotificationConfiguration",
        "notifications:GetManagedNotificationEvent",
        "notifications:ListManagedNotificationChildEvents",
        "notifications:ListManagedNotificationConfigurations",
        "notifications:ListManagedNotificationEvents",
        "organizations:*",
        "pricing:*",
        "q:*",
        "route53:*",
        "route53domains:*",
        "route53globalresolver:*",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "servicequotas:*",
        "signin:*",
        "sso-directory:*",
        "sso-oauth:*",
```

```
        "sso:*",
        "sts:*",
        "support:*",
        "tax:*",
        "trustedadvisor:*",
        "uxc:*",
        "waf:*",
        "wafv2:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "us-east-1"
        }
      }
    },
    {
      "Sid" : "DenyUsEast1WafResourceAssociation",
      "Effect" : "Deny",
      "Action" : [
        "wafv2:AssociateWebACL",
        "wafv2:DisassociateWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListResourcesForWebACL"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "us-east-1"
        }
      }
    },
    {
      "Sid" : "UsWest2Partitional",
      "Effect" : "Deny",
      "NotAction" : [
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:CreateInference",
        "bedrock-mantle:GetInference",
        "bedrock-mantle:GetModel",
        "bedrock-mantle:ListModels",
        "bedrock:ApplyGuardrail",
        "bedrock:CountTokens",
        "bedrock:GetFoundationModel",
```

```
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:ListFoundationModels",
        "bedrock:ListInferenceProfiles",
        "cloudshell:*",
        "cloudtrail:LookupEvents",
        "health:*",
        "identitystore-auth:*",
        "identitystore:*",
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:ListAliases",
        "networkmanager-chat:*",
        "networkmanager:*",
        "route53-recovery-cluster:*",
        "route53-recovery-control-config:*",
        "route53-recovery-readiness:*",
        "servicequotas:*",
        "sso-directory:*",
        "sso-oauth:*",
        "sso:*",
        "support:*",
        "trustedadvisor:*",
        "uxc:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "us-west-2"
        }
      }
    },
    {
      "Sid" : "RegionFloor",
      "Effect" : "Deny",
      "NotAction" : [
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:CreateInference",
        "bedrock-mantle:GetInference",
        "bedrock-mantle:GetModel",
        "bedrock-mantle:ListModels",
        "bedrock:ApplyGuardrail",
```

```
        "bedrock:CountTokens",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:ListFoundationModels",
        "bedrock:ListInferenceProfiles"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestedRegion" : [
            "unspecified",
            "us-east-1",
            "selected-region",
            "us-west-2"
          ]
        }
      }
    }
  ]
}
```

Après avoir activé les fonctionnalités avancées, la politique de contrôle des services suivante est appliquée à votre compte :

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "UsEast1Partitional",
      "Effect" : "Deny",
      "NotAction" : [
        "a4b:*",
        "access-analyzer:*",
        "account-access:*",
        "account:*",
        "acm:*",
        "activate:*",
        "artifact:*",
        "aws-marketplace-management:*",
        "aws-marketplace:*",
```

```
        "aws-portal:*",
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:CreateInference",
        "bedrock-mantle:GetInference",
        "bedrock-mantle:GetModel",
        "bedrock-mantle:ListModels",
        "bedrock:ApplyGuardrail",
        "bedrock:CountTokens",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:ListFoundationModels",
        "bedrock:ListInferenceProfiles",
        "billing:*",
        "billingconductor:*",
        "budgets:*",
        "builderid:*",
        "ce:*",
        "chatbot:*",
        "chime:*",
        "cloudfront-keyvaluestore:*",
        "cloudfront:*",
        "cloudshell:*",
        "cloudtrail:LookupEvents",
        "cloudwatch:BatchGet*",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "compute-optimizer:*",
        "config:*",
        "consoleapp:*",
        "consolidatedbilling:*",
        "cost-optimization-hub:*",
        "cur:*",
        "datapipeline:GetAccountLimits",
        "devicefarm:*",
        "directconnect:*",
        "ec2:DescribeRegions",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpnGateways",
        "ecr-public:*",
```

```
        "fms:*",
        "freetier:*",
        "globalaccelerator:*",
        "health:*",
        "iam:*",
        "identitystore-auth:*",
        "identitystore:*",
        "importexport:*",
        "invoicing:*",
        "iq:*",
        "kms:*",
        "license-manager:ListReceivedLicenses",
        "lightsail:AttachCertificateToDistribution",
        "lightsail:CreateCertificate",
        "lightsail:CreateContactMethod",
        "lightsail:CreateDistribution",
        "lightsail:CreateDomain",
        "lightsail:CreateDomainEntry",
        "lightsail:DeleteAlarm",
        "lightsail:DeleteCertificate",
        "lightsail:DeleteContactMethod",
        "lightsail:DeleteDistribution",
        "lightsail:DeleteDomain",
        "lightsail:DeleteDomainEntry",
        "lightsail:DetachCertificateFromDistribution",
        "lightsail:Get*",
        "lightsail:IsVpcPeered",
        "lightsail:PutAlarm",
        "lightsail:ResetDistributionCache",
        "lightsail:SendContactMethodVerification",
        "lightsail:SetIpAddressType",
        "lightsail:TagResource",
        "lightsail:TestAlarm",
        "lightsail:UntagResource",
        "lightsail:UpdateDistribution",
        "lightsail:UpdateDistributionBundle",
        "lightsail:UpdateDomainEntry",
        "logs:*",
        "managedblockchain-query:*",
        "managedblockchain:*",
        "mapcredits:*",
        "mobileanalytics:*",
        "networkmanager:*",
        "notifications-contacts:*",
```

```
        "notifications:*",
        "organizations:*",
        "payments:*",
        "pricing:*",
        "q:*",
        "quicksight:DescribeAccountSubscription",
        "resource-explorer-2:*",
        "route53-recovery-cluster:*",
        "route53-recovery-control-config:*",
        "route53-recovery-readiness:*",
        "route53:*",
        "route53domains:*",
        "route53globalresolver:*",
        "s3:CreateMultiRegionAccessPoint",
        "s3:DeleteMultiRegionAccessPoint",
        "s3:DescribeMultiRegionAccessPointOperation",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensDashboard",
        "s3:ListAllMyBuckets",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3:PutAccountPublicAccessBlock",
        "s3:PutMultiRegionAccessPointPolicy",
        "savingsplans:*",
        "servicequotas:*",
        "shield:*",
        "signin:*",
        "sso-directory:*",
        "sso-oauth:*",
        "sso:*",
        "sts:*",
        "support:*",
        "supportapp:*",
        "supportplans:*",
        "sustainability:*",
        "tag:GetResources",
        "tax:*",
```

```
        "trustedadvisor:*",
        "uxc:*",
        "vendor-insights:ListEntitledSecurityProfiles",
        "waf-regional:*",
        "waf:*",
        "wafv2:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "us-east-1"
        }
      }
    },
    {
      "Sid" : "UsWest2Partitional",
      "Effect" : "Deny",
      "NotAction" : [
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:CreateInference",
        "bedrock-mantle:GetInference",
        "bedrock-mantle:GetModel",
        "bedrock-mantle:ListModels",
        "bedrock:ApplyGuardrail",
        "bedrock:CountTokens",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:ListFoundationModels",
        "bedrock:ListInferenceProfiles",
        "cloudshell:*",
        "cloudtrail:LookupEvents",
        "health:*",
        "identitystore-auth:*",
        "identitystore:*",
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:ListAliases",
        "networkmanager-chat:*",
        "networkmanager:*",
        "route53-recovery-cluster:*",
        "route53-recovery-control-config:*",
```

```
        "route53-recovery-readiness:*",
        "servicequotas:*",
        "sso-directory:*",
        "sso-oauth:*",
        "sso:*",
        "support:*",
        "trustedadvisor:*",
        "uxc:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "us-west-2"
        }
      }
    },
    {
      "Sid" : "RegionFloor",
      "Effect" : "Deny",
      "NotAction" : [
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:CreateInference",
        "bedrock-mantle:GetInference",
        "bedrock-mantle:GetModel",
        "bedrock-mantle:ListModels",
        "bedrock:ApplyGuardrail",
        "bedrock:CountTokens",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:ListFoundationModels",
        "bedrock:ListInferenceProfiles"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestedRegion" : [
            "unspecified",
            "us-east-1",
            "selected-region",
            "us-west-2"
          ]
```

```
        }
      }
    }
  ]
}
```

Politiques de contrôle des services pour les limites de dépenses

Si vous utilisez une limite de dépenses, les politiques de contrôle des services suivantes sont appliquées à votre projet lorsqu'il approche de la limite de dépenses. Pour plus d'informations sur les limites de dépenses, consultezCréez une limite de dépenses dans AWS Settings.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "DenyBedrockUsage",
    "Effect": "Deny",
    "Action": [
      "bedrock:ApplyGuardrail",
      "bedrock:CallWithBearerToken",
      "bedrock:InvokeAgent",
      "bedrock:InvokeAutomatedReasoningPolicy",
      "bedrock:InvokeDataAutomation",
      "bedrock:InvokeDataAutomationAsync",
      "bedrock:InvokeFlow",
      "bedrock:InvokeInlineAgent",
      "bedrock:InvokeModel",
      "bedrock:InvokeModelWithResponseStream",
      "bedrock:InvokeTool",
      "bedrock:OptimizePrompt",
      "bedrock:Retrieve",
      "bedrock:RetrieveAndGenerate",
      "bedrock:StartFlowExecution",
      "bedrock-mantle:CallWithBearerToken",
      "bedrock-mantle:CreateInference"
    ],
    "Resource": "*"
  }
}
```

```
{
  "Version": "2012-10-17",
```

```
  "Statement": {
    "Sid": "DenyLambdaUsage",
    "Effect": "Deny",
    "Action": [
      "lambda:DeleteFunctionConcurrency",
      "lambda:InvokeAsync",
      "lambda:InvokeFunction",
      "lambda:InvokeFunctionUrl",
      "lambda:PutFunctionConcurrency"
    ],
    "Resource": "*"
  }
}
```

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "DenySageMakerInference",
    "Effect": "Deny",
    "Action": [
      "sagemaker:InvokeEndpoint",
      "sagemaker:InvokeEndpointAsync",
      "sagemaker:InvokeEndpointWithResponseStream"
    ],
    "Resource": "*"
  }
}
```

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyCompute",
      "Effect": "Deny",
      "Action": [
        "ec2:CreateNatGateway",
        "ec2:CreateVolume",
        "ec2:CreateVpnConnection",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "elasticloadbalancing:CreateLoadBalancer",
        "autoscaling:CreateAutoScalingGroup",
        "ecs:CreateService",
```

```
        "eks:CreateCluster",
        "eks:CreateNodegroup",
        "eks:CreateFargateProfile",
        "elasticbeanstalk:CreateEnvironment",
        "apprunner:CreateService",
        "apprunner:ResumeService",
        "batch:CreateComputeEnvironment",
        "elasticmapreduce:RunJobFlow",
        "appstream:CreateFleet"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyLambda",
      "Effect": "Deny",
      "Action": "lambda:CreateFunction",
      "Resource": "*"
    },
    {
      "Sid": "DenyDatabase",
      "Effect": "Deny",
      "Action": [
        "rds:CreateDBCluster",
        "rds:CreateDBInstance",
        "rds:RestoreDBClusterFromS3",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime",
        "rds:RestoreDBInstanceFromDBSnapshot",
        "rds:RestoreDBInstanceFromS3",
        "rds:RestoreDBInstanceToPointInTime",
        "rds:StartDBCluster",
        "rds:StartDBInstance",
        "dynamodb:CreateTable",
        "dynamodb:CreateGlobalTable",
        "elasticache:CreateCacheCluster",
        "elasticache:CreateReplicationGroup",
        "timestream:CreateDatabase",
        "timestream:CreateTable",
        "memorydb:CreateCluster",
        "es:CreateDomain",
        "aoss:CreateCollection",
        "redshift:CreateCluster",
        "redshift:ResumeCluster",
        "redshift-serverless:CreateWorkgroup",
```

```
        "dsql:CreateCluster"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyStorage",
      "Effect": "Deny",
      "Action": [
        "elasticfilesystem:CreateFileSystem",
        "datasync:CreateTask",
        "storagegateway:ActivateGateway",
        "glacier:CreateVault"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenySageMaker",
      "Effect": "Deny",
      "Action": [
        "sagemaker:CreateApp",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:StartNotebookInstance"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyBedrock",
      "Effect": "Deny",
      "Action": [
        "bedrock:CreateCustomModelDeployment",
        "bedrock:CreateDataAutomationProject",
        "bedrock:CreateEvaluationJob",
        "bedrock:CreateMarketplaceModelEndpoint",
        "bedrock:CreateModelCustomizationJob",
        "bedrock:CreateModelImportJob",
        "bedrock:CreateModelInvocationJob",
        "bedrock:CreateProvisionedModelThroughput",
        "bedrock-mantle:CreateCustomizedModel",
        "bedrock-mantle:CreateFineTuningJob",
        "bedrock-mantle:CreateReservation"
```

```
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyAIML",
      "Effect": "Deny",
      "Action": [
        "kendra:CreateIndex",
        "personalize:CreateSolution",
        "personalize:CreateCampaign",
        "forecast:CreatePredictor",
        "forecast:CreateForecast",
        "rekognition:CreateProject",
        "lex:CreateBot"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyNetworking",
      "Effect": "Deny",
      "Action": [
        "cloudfront:CreateDistribution",
        "route53:CreateHostedZone",
        "appmesh:CreateMesh"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyApiGatewayCreate",
      "Effect": "Deny",
      "Action": "apigateway:POST",
      "Resource": [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/apis"
      ]
    },
    {
      "Sid": "DenyMessaging",
      "Effect": "Deny",
      "Action": [
        "mq:CreateBroker",
        "kafka:CreateCluster",
        "kafka:CreateVpcConnection",
        "kinesis:CreateStream",
```

```
        "firehose:CreateDeliveryStream",
        "kinesisanalytics:CreateApplication",
        "kinesisvideo:CreateStream",
        "sns:CreateTopic",
        "sqs:CreateQueue",
        "events:CreateEventBus",
        "pipes:CreatePipe",
        "scheduler:CreateSchedule"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyAnalytics",
      "Effect": "Deny",
      "Action": [
        "states:CreateStateMachine",
        "glue:CreateJob",
        "glue:CreateCrawler",
        "athena:CreateWorkGroup",
        "appsync:CreateGraphqlApi",
        "appflow:CreateFlow",
        "datazone:CreateDomain",
        "datazone:CreateProject",
        "entityresolution:CreateMatchingWorkflow",
        "datapipeline:CreatePipeline",
        "dataexchange:CreateDataSet"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyDevTools",
      "Effect": "Deny",
      "Action": [
        "amplify:CreateApp",
        "amplify:CreateBranch",
        "cloud9:CreateEnvironmentEC2",
        "codebuild:CreateProject",
        "codepipeline:CreatePipeline",
        "codedeploy:CreateApplication",
        "cloudformation:CreateStack",
        "cloudformation:CreateStackSet",
        "codeartifact:CreateRepository",
        "codeartifact:CreateDomain"
      ],
```

```
      "Resource": "*"
    },
    {
      "Sid": "DenySecurity",
      "Effect": "Deny",
      "Action": [
        "kms:CreateKey",
        "wafv2:CreateWebACL",
        "cloudhsm:CreateCluster",
        "network-firewall:CreateFirewall",
        "secretsmanager:CreateSecret",
        "acm-pca:CreateCertificateAuthority",
        "cognito-idp:CreateUserPool",
        "cognito-identity:CreateIdentityPool",
        "ds:CreateDirectory",
        "ds:CreateMicrosoftAD",
        "fms:PutPolicy",
        "payment-cryptography:CreateKey"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyMedia",
      "Effect": "Deny",
      "Action": [
        "medialive:CreateChannel",
        "mediapackage:CreateChannel",
        "mediaconnect:CreateFlow",
        "mediatailor:CreateChannel"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyIoT",
      "Effect": "Deny",
      "Action": [
        "iot:CreateThing",
        "iot:CreateTopicRule",
        "iotevents:CreateDetectorModel",
        "iottwinmaker:CreateWorkspace",
        "iotsitewise:CreateAssetModel",
        "iotsitewise:CreatePortal",
        "iotfleetwise:CreateCampaign"
      ],
```

```
      "Resource": "*"
    },
    {
      "Sid": "DenyMisc",
      "Effect": "Deny",
      "Action": [
        "ses:CreateConfigurationSet",
        "ecr:CreateRepository",
        "aps:CreateWorkspace",
        "healthlake:CreateFHIRDatastore",
        "transfer:CreateServer",
        "managedblockchain:CreateNetwork",
        "managedblockchain:CreateMember",
        "route53-recovery-control-config:CreateCluster",
        "fis:CreateExperimentTemplate",
        "appfabric:CreateAppBundle",
        "appfabric:CreateIngestion",
        "b2bi:CreateProfile",
        "b2bi:CreateTransformer",
        "geo:CreateMap",
        "geo:CreatePlaceIndex",
        "geo:CreateTracker",
        "geo:CreateGeofenceCollection",
        "geo:CreateRouteCalculator"
      ],
      "Resource": "*"
    }
  ]
}
```

Politiques de contrôle des services pour le niveau gratuit pour les projets

La politique de contrôle des services suivante contrôle l'accès aux AWS services disponibles dans le niveau gratuit de notre nouvelle AWS expérience. Cette politique ne peut pas être modifiée. Pour accéder à des services supplémentaires, mettez à jour votre compte. Pour plus d'informations, consultez Mettez à jour votre compte dans AWS Settings.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowFreeTierServices",
      "Effect": "Deny",
```

```
      "NotAction": [
        "a2c:*",
        "access-analyzer:CheckAccessNotGranted",
        "access-analyzer:CheckNoNewAccess",
        "access-analyzer:CheckNoPublicAccess",
        "access-analyzer:ValidatePolicy",
        "account:*",
        "acm:*",
        "aco-automation:*",
        "action-recommendations:*",
        "activate:*",
        "aiops:*",
        "airflow-serverless:*",
        "amplify:*",
        "amplifybackend:*",
        "amplifyuibuilder:*",
        "aoss:*",
        "apigateway:*",
        "app-integrations:*",
        "appconfig:*",
        "appflow:*",
        "application-autoscaling:*",
        "application-signals-mcp:*",
        "application-signals:*",
        "application-transformation:*",
        "applicationinsights:*",
        "appmesh:*",
        "appsync:*",
        "aps:*",
        "arc-zonal-shift:*",
        "artifact:*",
        "athena:*",
        "autoscaling-plans:*",
        "autoscaling:*",
        "aws-external-anthropic:*",
        "aws-marketplace:*",
        "b2bi:*",
        "backup-gateway:*",
        "backup-search:*",
        "backup-storage:*",
        "backup:*",
        "batch:*",
        "bcm-pricing-calculator:*",
        "bedrock-agentcore:*",
```

```
        "bedrock-mantle:*",
        "bedrock-websearch:*",
        "bedrock:*",
        "budgets:*",
        "ce:*",
        "chatbot:*",
        "cloud9:*",
        "cloudformation:*",
        "cloudfront-keyvaluestore:*",
        "cloudfront:*",
        "cloudshell:*",
        "cloudtrail-data:*",
        "cloudtrail:*",
        "cloudwatch:*",
        "codeartifact:*",
        "codebuild:*",
        "codecommit:*",
        "codeconnections:*",
        "codedeploy-commands-secure:*",
        "codedeploy:*",
        "codepipeline:*",
        "codestar-connections:*",
        "codestar-notifications:*",
        "cognito-identity:*",
        "cognito-idp:*",
        "cognito-sync:*",
        "compute-optimizer:*",
        "config:*",
        "consoleapp:*",
        "consolidatedbilling:*",
        "cost-optimization-hub:*",
        "customer-verification:*",
        "databrew:*",
        "datapipeline:*",
        "datasync:*",
        "datazone:*",
        "dbqms:*",
        "dlm:*",
        "ds-data:*",
        "ds:*",
        "dsql:*",
        "dynamodb:*",
        "ebs:*",
        "ec2-instance-connect:*",
```

```
        "ec2:*",
        "ec2messages:*",
        "ecr-public:*",
        "ecr:*",
        "ecs-mcp:*",
        "ecs:*",
        "eks-auth:*",
        "eks-mcp:*",
        "eks:*",
        "elasticache:*",
        "elasticbeanstalk:*",
        "elasticfilesystem:*",
        "elasticloadbalancing:*",
        "entityresolution:*",
        "es:*",
        "events:*",
        "evidently:*",
        "execute-api:*",
        "finops-agent:*",
        "freertos:*",
        "freetier:*",
        "geo-maps:*",
        "geo-places:*",
        "geo-routes:*",
        "geo:*",
        "glue:*",
        "groundtruthlabeling:*",
        "health:*",
        "iam:*",
        "identitystore-auth:*",
        "identitystore:*",
        "imagebuilder:*",
        "internetmonitor:*",
        "invoicing:*",
        "iot-device-tester:*",
        "iot:*",
        "iotdeviceadvisor:*",
        "iotfleethub:*",
        "iotjobsdata:*",
        "iotmanagedintegrations:*",
        "iotsitewise:*",
        "iottwinmaker:*",
        "iotwireless:*",
        "kms:*",
```

```
        "lakeformation:*",
        "lambda:*",
        "launchwizard:*",
        "lex:*",
        "license-manager-linux-subscriptions:*",
        "license-manager-user-subscriptions:*",
        "license-manager:*",
        "logs:*",
        "mgn:*",
        "migrationhub-orchestrator:*",
        "migrationhub-strategy:*",
        "mpa:*",
        "mq:*",
        "networkflowmonitor:*",
        "networkmanager-chat:*",
        "networkmanager:*",
        "networkmonitor:*",
        "notifications-contacts:*",
        "notifications:*",
        "nova-act:*",
        "oam:*",
        "observabilityadmin:*",
        "opensearch:*",
        "organizations:*",
        "osis:*",
        "payment-cryptography:*",
        "pi:*",
        "pipes:*",
        "polly:*",
        "pricing:*",
        "q:DeleteConversation",
        "q:GenerateCodeFromCommands",
        "q:GenerateCodeRecommendations",
        "q:GetConversation",
        "q:GetIdentityMetadata",
        "q:GetTroubleshootingResults",
        "q:ListConversations",
        "q:PassRequest",
        "q:SendEvent",
        "q:SendMessage",
        "q:StartConversation",
        "q:StartTroubleshootingAnalysis",
        "q:StartTroubleshootingResolutionExplanation",
        "q:UpdateConversation",
```

```
        "q:UpdateTroubleshootingCommandResult",
        "q:UsePlugin",
        "ram:*",
        "rbin:*",
        "rds-data:*",
        "rds-db:*",
        "rds:*",
        "rekognition:*",
        "resource-explorer-2:*",
        "resource-explorer:*",
        "resource-groups:*",
        "rhelkb:*",
        "route53-recovery-cluster:*",
        "route53-recovery-control-config:*",
        "route53-recovery-readiness:*",
        "route53:*",
        "route53domains:*",
        "route53globalresolver:*",
        "route53profiles:*",
        "route53resolver:*",
        "rum:*",
        "s3-object-lambda:*",
        "s3:*",
        "s3express:*",
        "s3files:*",
        "s3tables:*",
        "s3vectors:*",
        "sagemaker-data-science-assistant:*",
        "sagemaker-geospatial:*",
        "sagemaker-mlflow:*",
        "sagemaker-unified-studio-mcp:*",
        "sagemaker:*",
        "scheduler:*",
        "schemas:*",
        "secretsmanager:*",
        "serverlessrepo:*",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
        "servicecatalog:ProvisionProduct",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct",
```

```
        "servicediscovery:*",
        "serviceextract:*",
        "servicequotas:*",
        "ses:*",
        "signer:*",
        "signin:*",
        "sns:*",
        "sqlworkbench:*",
        "sqs:*",
        "ssm-contacts:*",
        "ssm-guiconnect:*",
        "ssm-incidents:*",
        "ssm-quicksetup:*",
        "ssm-sap:*",
        "ssm:*",
        "ssmmessages:*",
        "sso-directory:*",
        "sso-oauth:*",
        "sso:*",
        "states:*",
        "sts:*",
        "support:*",
        "swf:*",
        "synthetics:*",
        "tag:*",
        "tax:*",
        "timestream-influxdb:*",
        "ts:*",
        "uxc:*",
        "verifiedpermissions:*",
        "vpce:*",
        "waf-regional:*",
        "waf:*",
        "wafv2:*",
        "wellarchitected:*",
        "xray:*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyEC2CapacityBlock",
      "Effect": "Deny",
      "Action": ["ec2:PurchaseCapacityBlock", "ec2:PurchaseCapacityBlockExtension"],
      "Resource": "*"
```

```
    },
    {
      "Sid": "DenyRestrictedAgreements",
      "Effect": "Deny",
      "Action": ["artifact:AcceptAgreement", "artifact:AcceptNdaForAgreement"],
      "Resource": [
        "arn:aws:artifact:::agreement/agreement-9c1kBcYznTkcpRIm",
        "arn:aws:artifact:::agreement/agreement-y03aUwMAEorHtqjv",
        "arn:aws:artifact:::agreement/agreement-bexgr7sjvXAW4Gxu",
        "arn:aws:artifact:::agreement/agreement-HZTdNwJuqOKLReXC"
      ]
    },
    {
      "Sid": "DenyDocDB",
      "Effect": "Deny",
      "Action": ["rds:CreateDBCluster", "rds:CreateDBInstance"],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "rds:DatabaseEngine": ["docdb"]
        }
      }
    },
    {
      "Sid": "DenyCloudWAN",
      "Effect": "Deny",
      "Action": [
        "networkmanager:CreateCoreNetwork",
        "networkmanager:CreateConnectAttachment",
        "networkmanager:CreateConnectPeer",
        "networkmanager:CreateVpcAttachment",
        "networkmanager:CreateSiteToSiteVpnAttachment",
        "networkmanager:CreateTransitGatewayPeering",
        "networkmanager:CreateDirectConnectGatewayAttachment",
        "networkmanager:PutCoreNetworkPolicy",
        "networkmanager:ExecuteCoreNetworkChangeSet"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyTransitGatewayAndVPN",
      "Effect": "Deny",
      "Action": [
        "ec2:CreateTransitGateway",
```

```
        "ec2:CreateTransitGatewayVpcAttachment",
        "ec2:CreateTransitGatewayConnect",
        "ec2:CreateTransitGatewayConnectPeer",
        "ec2:CreateTransitGatewayMulticastDomain",
        "ec2:CreateTransitGatewayPeeringAttachment",
        "ec2:CreateTransitGatewayPolicyTable",
        "ec2:CreateTransitGatewayPrefixListReference",
        "ec2:CreateTransitGatewayRoute",
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2:CreateClientVpnEndpoint",
        "ec2:CreateClientVpnRoute",
        "ec2:AuthorizeClientVpnIngress",
        "ec2:AssociateClientVpnTargetNetwork",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:CreateCustomerGateway"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenySageMakerGroundTruth",
      "Effect": "Deny",
      "Action": [
        "sagemaker:CreateLabelingJob",
        "sagemaker:CreateWorkteam",
        "sagemaker:CreateWorkforce",
        "sagemaker:CreateHumanTaskUi"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyGlacierStorageClasses",
      "Effect": "Deny",
      "Action": ["s3:PutObject"],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-storage-class": ["DEEP_ARCHIVE", "GLACIER"]
        }
      }
    },
    {
```

```
      "Sid": "DenyEC2Fleet",
      "Effect": "Deny",
      "Action": ["ec2:CreateFleet"],
      "Resource": "*"
    },
    {
      "Sid": "DenyEC2BYOLAndLicenseConfigurations",
      "Effect": "Deny",
      "Action": ["ec2:RunInstances", "ec2:StartInstances"],
      "Resource": "arn:aws:ec2:*:*:instance/*",
      "Condition": {
        "StringEquals": {
          "ec2:Tenancy": "host"
        }
      }
    },
    {
      "Sid": "DenyEC2InstanceStoreRootDevice",
      "Effect": "Deny",
      "Action": ["ec2:RunInstances"],
      "Resource": "arn:aws:ec2:*:*:instance/*",
      "Condition": {
        "StringEquals": {
          "ec2:RootDeviceType": "instance-store"
        }
      }
    },
    {
      "Sid": "DenyLicenseManagerAssociation",
      "Effect": "Deny",
      "Action": ["license-manager:CreateLicenseConfiguration"],
      "Resource": "*"
    },
    {
      "Sid": "DenyIAMRestrictedActions",
      "Effect": "Deny",
      "Action": [
        "iam:*Alias*",
        "iam:*Organizations*",
        "iam:*Provider*",
        "iam:SetSecurityTokenServicePreferences",
        "iam:*LoginProfile*",
        "iam:CreateGroup",
        "iam:AttachGroupPolicy",
```

```
        "iam:AddUserToGroup",
        "iam:PutGroupPolicy",
        "iam:UpdateGroup",
        "iam:UpdateServerCertificate",
        "iam:UpdateSigningCertificate",
        "iam:UploadServerCertificate",
        "iam:UploadSigningCertificate",
        "iam:TagServerCertificate",
        "iam:UntagServerCertificate"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenySSOCreateInstance",
      "Effect": "Deny",
      "Action": ["sso:CreateInstance"],
      "Resource": "*"
    },
    {
      "Sid": "DenyRequestSpotInstances",
      "Effect": "Deny",
      "Action": ["ec2:RequestSpotInstances"],
      "Resource": "*"
    },
    {
      "Sid": "DenySpotMarketType",
      "Effect": "Deny",
      "Action": ["ec2:RunInstances"],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:InstanceMarketType": "spot"
        }
      }
    },
    {
      "Sid": "DenyReservedInstanceAndCapacityPurchases",
      "Effect": "Deny",
      "Action": [
        "athena:CreateCapacityReservation",
        "cloudfront:CreateSavingsPlan",
        "dynamodb:PurchaseReservedCapacityOfferings",
        "ec2:AllocateHosts",
        "ec2:CreateCapacityReservation",
```

```
        "ec2:CreateCapacityReservationBySplitting",
        "ec2:CreateCapacityReservationCancellationQuote",
        "ec2:CreateCapacityReservationFleet",
        "ec2:PurchaseHostReservation",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:PurchaseScheduledInstances",
        "elasticache:PurchaseReservedCacheNodesOffering",
        "es:PurchaseReservedElasticsearchInstanceOffering",
        "es:PurchaseReservedInstanceOffering",
        "glacier:PurchaseProvisionedCapacity",
        "memorydb:PurchaseReservedNodesOffering",
        "rds:PurchaseReservedDBInstancesOffering",
        "redshift:AcceptReservedNodeExchange",
        "redshift:PurchaseReservedNodeOffering",
        "sagemaker:CreateReservedCapacity",
        "savingsplans:CreateSavingsPlan"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyExportableCertificateRequests",
      "Effect": "Deny",
      "Action": ["acm:RequestCertificate"],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "acm:AllowExport": "true"
        }
      }
    }
  ]
}
```

Politiques de contrôle des services pour le plan payant pour les projets

La politique de contrôle des services suivante contrôle l'accès aux AWS services disponibles dans le plan payant de notre nouvelle AWS expérience. Cette politique ne peut pas être modifiée. Pour accéder à des services supplémentaires, activez les fonctionnalités avancées. Pour plus d'informations, consultez Activer le mode avancé AWS fonctionnalités.

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

```
    {
      "Sid": "AllowPaidTierServices",
      "Effect": "Deny",
      "NotAction": [
        "a2c:*",
        "access-analyzer:CheckAccessNotGranted",
        "access-analyzer:CheckNoNewAccess",
        "access-analyzer:CheckNoPublicAccess",
        "access-analyzer:ValidatePolicy",
        "account:*",
        "acm:*",
        "aco-automation:*",
        "action-recommendations:*",
        "activate:*",
        "aidevops:*",
        "aiops:*",
        "airflow-serverless:*",
        "amplify:*",
        "amplifybackend:*",
        "amplifyuibuilder:*",
        "aoss:*",
        "apigateway:*",
        "app-integrations:*",
        "appconfig:*",
        "appfabric:*",
        "appflow:*",
        "application-autoscaling:*",
        "application-signals-mcp:*",
        "application-signals:*",
        "application-transformation:*",
        "applicationinsights:*",
        "appmesh:*",
        "appsync:*",
        "aps:*",
        "arc-zonal-shift:*",
        "artifact:*",
        "athena:*",
        "autoscaling-plans:*",
        "autoscaling:*",
        "aws-external-anthropic:*",
        "aws-marketplace:*",
        "b2bi:*",
        "backup-gateway:*",
        "backup-search:*",
```

```
        "backup-storage:*",
        "backup:*",
        "batch:*",
        "bcm-pricing-calculator:*",
        "bedrock-agentcore:*",
        "bedrock-mantle:*",
        "bedrock-websearch:*",
        "bedrock:*",
        "budgets:*",
        "ce:*",
        "chatbot:*",
        "cloud9:*",
        "cloudformation:*",
        "cloudfront-keyvaluestore:*",
        "cloudfront:*",
        "cloudshell:*",
        "cloudtrail-data:*",
        "cloudtrail:*",
        "cloudwatch:*",
        "codeartifact:*",
        "codebuild:*",
        "codecommit:*",
        "codeconnections:*",
        "codedeploy-commands-secure:*",
        "codedeploy:*",
        "codeguru-profiler:*",
        "codeguru-reviewer:*",
        "codeguru-security:*",
        "codepipeline:*",
        "codestar-connections:*",
        "codestar-notifications:*",
        "cognito-identity:*",
        "cognito-idp:*",
        "cognito-sync:*",
        "compute-optimizer:*",
        "config:*",
        "consoleapp:*",
        "consolidatedbilling:*",
        "cost-optimization-hub:*",
        "customer-verification:*",
        "databrew:*",
        "dataexchange:*",
        "datapipeline:*",
        "datasync:*",
```

```
        "datazone:*",
        "dbqms:*",
        "devops-guru:*",
        "dlm:*",
        "docdb-elastic:*",
        "ds-data:*",
        "ds:*",
        "dsql:*",
        "dynamodb:*",
        "ebs:*",
        "ec2-instance-connect:*",
        "ec2:*",
        "ec2messages:*",
        "ecr-public:*",
        "ecr:*",
        "ecs-mcp:*",
        "ecs:*",
        "eks-auth:*",
        "eks-mcp:*",
        "eks:*",
        "elasticache:*",
        "elasticbeanstalk:*",
        "elasticfilesystem:*",
        "elasticloadbalancing:*",
        "elasticmapreduce:*",
        "emr-containers:*",
        "emr-serverless:*",
        "entityresolution:*",
        "es:*",
        "events:*",
        "evidently:*",
        "execute-api:*",
        "finops-agent:*",
        "firehose:*",
        "fis:*",
        "fms:*",
        "forecast:*",
        "freertos:*",
        "freetier:*",
        "geo-maps:*",
        "geo-places:*",
        "geo-routes:*",
        "geo:*",
        "glacier:*",
```

```
        "glue:*",
        "groundtruthlabeling:*",
        "health:*",
        "iam:*",
        "identitystore-auth:*",
        "identitystore:*",
        "imagebuilder:*",
        "internetmonitor:*",
        "invoicing:*",
        "iot-device-tester:*",
        "iot:*",
        "iotdeviceadvisor:*",
        "iotfleethub:*",
        "iotjobsdata:*",
        "iotmanagedintegrations:*",
        "iotsitewise:*",
        "iottwinmaker:*",
        "iotwireless:*",
        "kafka-cluster:*",
        "kafka:*",
        "kafkaconnect:*",
        "kinesis:*",
        "kinesisanalytics:*",
        "kinesisvideo:*",
        "kms:*",
        "lakeformation:*",
        "lambda:*",
        "launchwizard:*",
        "lex:*",
        "license-manager-linux-subscriptions:*",
        "license-manager-user-subscriptions:*",
        "license-manager:*",
        "logs:*",
        "managedblockchain-query:*",
        "managedblockchain:*",
        "mapcredits:*",
        "memorydb:*",
        "mgn:*",
        "migrationhub-orchestrator:*",
        "migrationhub-strategy:*",
        "mpa:*",
        "mq:*",
        "neptune-db:*",
        "neptune-graph:*",
```

```
        "network-firewall:*",
        "networkflowmonitor:*",
        "networkmanager-chat:*",
        "networkmanager:*",
        "networkmonitor:*",
        "notifications-contacts:*",
        "notifications:*",
        "nova-act:*",
        "oam:*",
        "observabilityadmin:*",
        "opensearch:*",
        "organizations:*",
        "osis:*",
        "payment-cryptography:*",
        "personalize:*",
        "pi:*",
        "pipes:*",
        "polly:*",
        "pricing:*",
        "q:DeleteConversation",
        "q:GenerateCodeFromCommands",
        "q:GenerateCodeRecommendations",
        "q:GetConversation",
        "q:GetIdentityMetadata",
        "q:GetTroubleshootingResults",
        "q:ListConversations",
        "q:PassRequest",
        "q:SendEvent",
        "q:SendMessage",
        "q:StartConversation",
        "q:StartTroubleshootingAnalysis",
        "q:StartTroubleshootingResolutionExplanation",
        "q:UpdateConversation",
        "q:UpdateTroubleshootingCommandResult",
        "q:UsePlugin",
        "ram:*",
        "rbin:*",
        "rds-data:*",
        "rds-db:*",
        "rds:*",
        "redshift-data:*",
        "redshift-serverless:*",
        "redshift:*",
        "rekognition:*",
```

```
        "resource-explorer-2:*",
        "resource-explorer:*",
        "resource-groups:*",
        "rhelkb:*",
        "route53-recovery-cluster:*",
        "route53-recovery-control-config:*",
        "route53-recovery-readiness:*",
        "route53:*",
        "route53domains:*",
        "route53globalresolver:*",
        "route53profiles:*",
        "route53resolver:*",
        "rum:*",
        "s3-object-lambda:*",
        "s3:*",
        "s3express:*",
        "s3files:*",
        "s3tables:*",
        "s3vectors:*",
        "sagemaker-data-science-assistant:*",
        "sagemaker-geospatial:*",
        "sagemaker-mlflow:*",
        "sagemaker-unified-studio-mcp:*",
        "sagemaker:*",
        "scheduler:*",
        "schemas:*",
        "secretsmanager:*",
        "securityagent:*",
        "serverlessrepo:*",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
        "servicecatalog:ProvisionProduct",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct",
        "servicediscovery:*",
        "serviceextract:*",
        "servicequotas:*",
        "ses:*",
        "signer:*",
        "signin:*",
        "sms-voice:*",
```

```
        "sns:*",
        "social-messaging:*",
        "sqlworkbench:*",
        "sqs:*",
        "ssm-contacts:*",
        "ssm-guiconnect:*",
        "ssm-incidents:*",
        "ssm-quicksetup:*",
        "ssm-sap:*",
        "ssm:*",
        "ssmmessages:*",
        "sso-directory:*",
        "sso-oauth:*",
        "sso:*",
        "states:*",
        "storagegateway:*",
        "sts:*",
        "support:*",
        "swf:*",
        "synthetics:*",
        "tag:*",
        "tax:*",
        "textract:*",
        "timestream-influxdb:*",
        "timestream:*",
        "transcribe:*",
        "translate:*",
        "ts:*",
        "uxc:*",
        "verifiedpermissions:*",
        "vpce:*",
        "waf-regional:*",
        "waf:*",
        "wafv2:*",
        "wellarchitected:*",
        "xray:*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyEC2CapacityBlock",
      "Effect": "Deny",
      "Action": ["ec2:PurchaseCapacityBlock", "ec2:PurchaseCapacityBlockExtension"],
      "Resource": "*"
```

```
    },
    {
      "Sid": "DenyRestrictedAgreements",
      "Effect": "Deny",
      "Action": ["artifact:AcceptAgreement", "artifact:AcceptNdaForAgreement"],
      "Resource": [
        "arn:aws:artifact:::agreement/agreement-9c1kBcYznTkcpRIm",
        "arn:aws:artifact:::agreement/agreement-y03aUwMAEorHtqjv",
        "arn:aws:artifact:::agreement/agreement-bexgr7sjvXAW4Gxu",
        "arn:aws:artifact:::agreement/agreement-HZTdNwJuqOKLReXC"
      ]
    },
    {
      "Sid": "DenyCloudWAN",
      "Effect": "Deny",
      "Action": [
        "networkmanager:CreateCoreNetwork",
        "networkmanager:CreateConnectAttachment",
        "networkmanager:CreateConnectPeer",
        "networkmanager:CreateVpcAttachment",
        "networkmanager:CreateSiteToSiteVpnAttachment",
        "networkmanager:CreateTransitGatewayPeering",
        "networkmanager:CreateDirectConnectGatewayAttachment",
        "networkmanager:PutCoreNetworkPolicy",
        "networkmanager:ExecuteCoreNetworkChangeSet"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyTransitGatewayAndVPN",
      "Effect": "Deny",
      "Action": [
        "ec2:CreateTransitGateway",
        "ec2:CreateTransitGatewayVpcAttachment",
        "ec2:CreateTransitGatewayConnect",
        "ec2:CreateTransitGatewayConnectPeer",
        "ec2:CreateTransitGatewayMulticastDomain",
        "ec2:CreateTransitGatewayPeeringAttachment",
        "ec2:CreateTransitGatewayPolicyTable",
        "ec2:CreateTransitGatewayPrefixListReference",
        "ec2:CreateTransitGatewayRoute",
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2:CreateClientVpnEndpoint",
```

```
        "ec2:CreateClientVpnRoute",
        "ec2:AuthorizeClientVpnIngress",
        "ec2:AssociateClientVpnTargetNetwork",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:CreateCustomerGateway"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenySageMakerGroundTruth",
      "Effect": "Deny",
      "Action": [
        "sagemaker:CreateLabelingJob",
        "sagemaker:CreateWorkteam",
        "sagemaker:CreateWorkforce",
        "sagemaker:CreateHumanTaskUi"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyEC2Fleet",
      "Effect": "Deny",
      "Action": ["ec2:CreateFleet"],
      "Resource": "*"
    },
    {
      "Sid": "DenyEC2BYOLAndLicenseConfigurations",
      "Effect": "Deny",
      "Action": ["ec2:RunInstances", "ec2:StartInstances"],
      "Resource": "arn:aws:ec2:*:*:instance/*",
      "Condition": {
        "StringEquals": {
          "ec2:Tenancy": "host"
        }
      }
    },
    {
      "Sid": "DenyEC2InstanceStoreRootDevice",
      "Effect": "Deny",
      "Action": ["ec2:RunInstances"],
      "Resource": "arn:aws:ec2:*:*:instance/*",
      "Condition": {
```

```
        "StringEquals": {
          "ec2:RootDeviceType": "instance-store"
        }
      }
    },
    {
      "Sid": "DenyLicenseManagerAssociation",
      "Effect": "Deny",
      "Action": ["license-manager:CreateLicenseConfiguration"],
      "Resource": "*"
    },
    {
      "Sid": "DenyIAMRestrictedActions",
      "Effect": "Deny",
      "Action": [
        "iam:*Alias*",
        "iam:*Organizations*",
        "iam:*Provider*",
        "iam:SetSecurityTokenServicePreferences",
        "iam:*LoginProfile*",
        "iam:CreateGroup",
        "iam:AttachGroupPolicy",
        "iam:AddUserToGroup",
        "iam:PutGroupPolicy",
        "iam:UpdateGroup",
        "iam:UpdateServerCertificate",
        "iam:UpdateSigningCertificate",
        "iam:UploadServerCertificate",
        "iam:UploadSigningCertificate",
        "iam:TagServerCertificate",
        "iam:UntagServerCertificate"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenySSOCreateInstance",
      "Effect": "Deny",
      "Action": ["sso:CreateInstance"],
      "Resource": "*"
    },
    {
      "Sid": "DenyRequestSpotInstances",
      "Effect": "Deny",
      "Action": ["ec2:RequestSpotInstances"],
```

```
      "Resource": "*"
    },
    {
      "Sid": "DenySpotMarketType",
      "Effect": "Deny",
      "Action": ["ec2:RunInstances"],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:InstanceMarketType": "spot"
        }
      }
    },
    {
      "Sid": "DenyReservedInstanceAndCapacityPurchases",
      "Effect": "Deny",
      "Action": [
        "athena:CreateCapacityReservation",
        "cloudfront:CreateSavingsPlan",
        "dynamodb:PurchaseReservedCapacityOfferings",
        "ec2:AllocateHosts",
        "ec2:CreateCapacityReservation",
        "ec2:CreateCapacityReservationBySplitting",
        "ec2:CreateCapacityReservationCancellationQuote",
        "ec2:CreateCapacityReservationFleet",
        "ec2:PurchaseHostReservation",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:PurchaseScheduledInstances",
        "elasticache:PurchaseReservedCacheNodesOffering",
        "es:PurchaseReservedElasticsearchInstanceOffering",
        "es:PurchaseReservedInstanceOffering",
        "glacier:PurchaseProvisionedCapacity",
        "memorydb:PurchaseReservedNodesOffering",
        "rds:PurchaseReservedDBInstancesOffering",
        "redshift:AcceptReservedNodeExchange",
        "redshift:PurchaseReservedNodeOffering",
        "sagemaker:CreateReservedCapacity",
        "savingsplans:CreateSavingsPlan"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyExportableCertificateRequests",
      "Effect": "Deny",
```

```
      "Action": ["acm:RequestCertificate"],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "acm:AllowExport": "true"
        }
      }
    }
  ]
}
```

Politiques de contrôle des ressources pour les projets

Voici la politique de contrôle des ressources pour les ressources du projet. Cette politique ne peut pas être modifiée :

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DenyAnyoneOutsideMyOrgAndAWS",
      "Effect" : "Deny",
      "Principal" : "*",
      "Action" : [
        "aoss:*",
        "appconfig:*",
        "appstream:*",
        "autoscaling:*",
        "codebuild:*",
        "codecommit:*",
        "cognito-identity:*",
        "cognito-idp:*",
        "comprehend:*",
        "comprehendmedical:*",
        "dax:*",
        "dynamodb:*",
        "ecr:*",
        "health:*",
        "kinesisvideo:*",
        "kms:*",
        "logs:*",
        "s3:*",
        "secretsmanager:*",
```

```
        "sqs:*",
        "sts:*",
        "support:*",
        "textract:*",
        "transcribe:*",
        "translate:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "BoolIfExists" : {
          "aws:PrincipalIsAWSService" : "false"
        },
        "Null" : {
          "aws:PrincipalARN" : "false"
        },
        "StringNotEqualsIfExists" : {
          "aws:PrincipalOrgID" : "${aws:ResourceOrgID}"
        }
      }
    },
    {
      "Sid" : "DenyAWSWhenItsNotMyOrgsSourceAccount",
      "Effect" : "Deny",
      "Principal" : "*",
      "Action" : [
        "aoss:*",
        "appconfig:*",
        "appstream:*",
        "autoscaling:*",
        "codebuild:*",
        "codecommit:*",
        "cognito-identity:*",
        "cognito-idp:*",
        "comprehend:*",
        "comprehendmedical:*",
        "dax:*",
        "dynamodb:*",
        "ecr:*",
        "health:*",
        "kinesisvideo:*",
        "kms:*",
        "logs:*",
        "s3:*",
        "secretsmanager:*",
```

```
        "sqs:*",
        "sts:*",
        "support:*",
        "textract:*",
        "transcribe:*",
        "translate:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:SourceAccount" : "false"
        },
        "StringNotEquals" : {
          "aws:SourceOrgID" : "${aws:ResourceOrgID}"
        }
      }
    }
  ]
}
```

Basculer entre les projets

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Vous ne pouvez gérer les AWS ressources que pour un seul projet à la fois. Vous pouvez toujours savoir dans quel projet vous vous trouvez en vous basant sur le nom en haut à droite de la AWS console.

Passez d'un projet à l'autre pour les sessions actives à partir du Console de gestion AWS

Pour passer d'un projet à l'autre pour les sessions actives, depuis le Console de gestion AWS

1. Ouvrez la Console de gestion AWS.
2. Choisissez le nom de votre projet en haut à droite du Console de gestion AWS.
3. Choisissez le projet Switch.

4. Sous Sessions actives, choisissez une session active. Une session active est une session qui est connectée depuis 12 heures au maximum. L'heure de la session active ne peut pas être modifiée.
5. Vous serez redirigé vers la page d'accueil de la AWS console pour votre nouveau projet.

Passez d'un projet à l'autre dans AWS Settings

Pour passer d'un projet à l'autre dans AWS Settings

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez le projet auquel vous souhaitez accéder.
3. Dans la barre de navigation en haut à droite, choisissez Créer et gérer une infrastructure cloud.

   Vous serez redirigé vers la page correspondant Console de gestion AWS à votre nouveau projet.

Passez d'un projet à l'autre depuis Console de gestion AWS

Pour passer d'un projet à l'autre à partir du Console de gestion AWS

1. Ouvrez la Console de gestion AWS.
2. Choisissez Gérer les projets.
3. Dans AWS Paramètres, choisissez le projet auquel vous souhaitez accéder.
4. Dans la barre de navigation en haut à droite, choisissez Créer et gérer une infrastructure cloud.

   Vous serez redirigé vers la page correspondant Console de gestion AWS à votre nouveau projet.

Invitez les membres de l'équipe à collaborer AWS Settings

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Vous pouvez autoriser les membres de l'équipe à accéder à vos projets. Lorsque vous partagez un projet avec un membre de l'équipe, vous ne pouvez pas contrôler AWS les services auxquels il a

accès. Vous et le membre de l'équipe disposez d'un accès administrateur au projet. Cela signifie que le membre de l'équipe est autorisé à accéder à tous les AWS services disponibles pour votre projet. Cela inclut la création de contrôles d'accès pour les services et les applications. Cependant, ils ne sont pas autorisés à effectuer des actions administratives ou financières, telles que la suppression de votre projet ou la modification d'une limite de dépenses. Pour voir quel membre de l'équipe a modifié un AWS service, consultezSurveillez votre projet à l'aide de AWS CloudTrail.

Dans AWS Paramètres, vous et les membres de votre équipe disposez de différents niveaux d'accès. Pour consulter la politique AWS gérée appliquée à un membre de l'équipe, consultez AWSManagedSettingsReadOnlyAccess. Pour consulter la politique AWS gérée appliquée à un propriétaire de projet, consultez AWSManagedSettingsAdminAccess.

Tenez compte des points suivants lorsque vous ajoutez un membre de l'équipe à votre projet.

Considérations pour les membres de l'équipe

Un membre de l'équipe peut effectuer les actions suivantes :

- Afficher, créer, modifier, supprimer et modifier les AWS ressources d'un projet.
- AWS Paramètres d'accès.
- Consultez les limites de dépenses.
- Demandez une augmentation de quota pour un AWS service.

Un membre de l'équipe ne peut pas effectuer les actions suivantes :

- Quittez un projet.
- Effectuez toutes les actions root. Pour de plus amples informations, veuillez consulter AWS actions pour les porteurs de projets.
- Invitez les membres de l'équipe à participer à des projets.
- Gérez les autorisations de tous les membres de l'équipe.
- Supprimez un membre de l'équipe d'un projet.
- Changez le nom d'un projet.
- Configurez ou mettez à jour les modes de paiement.
- Consultez ou mettez à jour les informations de facturation, y compris l'adresse ou le numéro de téléphone.
- Consultez ou mettez à jour les informations fiscales.

- Passez du niveau gratuit au plan payant.
- Définissez ou modifiez les limites de dépenses par projet.
- Consultez l'évolution des coûts pour chaque projet.
- Consultez le total AWS des dépenses pour tous les projets.
- Consultez et échangez les crédits promotionnels du niveau non gratuit.
- Consultez les crédits restants et les dates d'expiration pour tous les types de crédits.
- Consultez l'historique de crédit complet, y compris les crédits gagnés, appliqués et expirés.
- Découvrez comment les crédits s'appliquent à l'ensemble des projets.
- Afficher le solde impayé.
- Exécutez des paiements à AWS.
- Téléchargez les factures ou consultez les transactions passées.
- Vérifiez que les AWS frais sont corrects, y compris les crédits appliqués.
- Recevez des communications de facturation au niveau du compte de gestion.
- Obtenez de l'aide pour résoudre les problèmes de facturation au niveau de l'organisation.
- Demandez une augmentation de quota pour les quotas de compte et de facturation.

Comment les membres de l'équipe accèdent à votre AWS resources

Notre nouvelle AWS expérience crée un rôle lié aux services pour l'organisation qui contient tous vos projets que vous ne pouvez pas modifier. Ce rôle vérifie périodiquement que les dossiers internes des membres de votre équipe restent synchronisés avec ceux des membres actuels de votre équipe.

Le rôle lié à un service AWSServiceRoleForAccountAccessManager approuve les services suivants pour endosser le rôle :

- `account-access.amazonaws.com`

La politique d'autorisations de rôle nommée `AccountAccessManagerServiceRolePolicy` permet au gestionnaire d'accès au compte d'effectuer les actions suivantes sur les ressources spécifiées :

- Action :`organizations:ListAccounts`,`organizations:ListAWSServiceAccessForOrganizat`
  `organizations:DescribeAccount` sur `"arn:aws:organizations::*:account/o-*/*"`

Pour plus d'informations, consultez AWS Account Access Manager.

Invitez les membres de l'équipe à collaborer AWS Settings

Pour inviter des membres de l'équipe, vous leur envoyez une invitation depuis la page Équipe des AWS paramètres. Les membres de l'équipe ont 14 jours pour accepter leur invitation. Les membres de l'équipe doivent créer un ID de constructeur AWS pour accéder à votre projet. Ils peuvent le faire en utilisant Sign up for AWS (new).

Invitez les membres de l'équipe à collaborer AWS Settings

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Team.
3. Choisissez Inviter un nouveau membre de l'équipe.
4. Dans le champ E-mail, saisissez une adresse e-mail ou une liste d'adresses e-mail. Séparez les adresses e-mail par des virgules (,) ou des points-virgules (;).
5. Choisissez un ou plusieurs projets à partager avec les nouveaux membres de votre équipe.
6. Choisissez Send invitation (Envoyer une invitation).

Si les membres de votre équipe ne reçoivent pas l'invitation, demandez-leur de vérifier leurs dossiers de courrier indésirable et de corbeille.

Inviter un membre de l'équipe à participer à un projet dans AWS Settings

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Vous pouvez inviter un membre de l'équipe à accéder à un projet. Pour plus d'informations sur ce que les membres de l'équipe peuvent faire dans le cadre d'un projet, consultezInvitez les membres de l'équipe à collaborer AWS Settings.

Pour inviter un membre de l'équipe à rejoindre un projet

1. Ouvrez AWS les paramètres sur https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez le projet auquel vous souhaitez accéder.
3. Pour Membres, choisissez Inviter un nouveau membre de l'équipe.
4. Pour E-mail, entrez une adresse e-mail ou une liste d'adresses e-mail. Séparez les adresses e-mail par des virgules (,) ou des points-virgules (;).
5. Choisissez un projet à partager avec les nouveaux membres de votre équipe.
6. Choisissez Send invitation (Envoyer une invitation).

Si les membres de votre équipe ne reçoivent pas l'invitation, demandez-leur de vérifier leurs dossiers de courrier indésirable et de corbeille.

Supprimer un membre de l'équipe d'un projet dans AWS Settings

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Vous pouvez supprimer un membre de l'équipe d'un projet à tout moment. Les membres de votre équipe ne peuvent pas le faire seuls. Lorsque vous supprimez un membre de l'équipe, il n'a plus accès à ce projet. Toutes les ressources créées par un membre de votre équipe restent dans votre projet et vous devez les gérer.

Pour supprimer un membre de l'équipe dans un projet

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez le projet auquel vous souhaitez accéder.
3. Dans l'onglet Membres, sélectionnez le membre avec lequel vous souhaitez supprimer du projet, puis choisissez Supprimer.
4. Confirmez votre choix et choisissez Supprimer.

Le membre de l'équipe fait toujours partie de votre équipe et vous pouvez l'ajouter à d'autres projets. Pour supprimer complètement un membre de l'équipe des AWS paramètres, consultezSupprimer un membre de l'équipe dans AWS Settings.

Supprimer un membre de l'équipe dans AWS Settings

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Vous pouvez utiliser la page Équipe pour supprimer un membre de l'équipe de tous les projets. Ils perdront automatiquement l'accès à tous les projets. Les ressources créées par le membre de l'équipe ne seront pas supprimées.

Pour supprimer un membre de l'équipe

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Team.
3. Cochez la case correspondant au membre de l'équipe que vous souhaitez supprimer.
4. Cliquez sur Supprimer.
5. Confirmez votre choix et choisissez Supprimer.

Révoquer une invitation adressée à un membre de l'équipe dans AWS Settings

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Vous pouvez révoquer une invitation en attente. L'invitation restera dans AWS les paramètres pendant 14 jours. Lorsque vous révoquez une invitation en attente, le lien d'accès contenu dans l'e-

mail d'invitation est désactivé. Vous ne pouvez pas révoquer une invitation acceptée, mais supprimer le membre de l'équipe. Pour de plus amples informations, veuillez consulter Supprimer un membre de l'équipe dans AWS Settings.

Pour révoquer une invitation

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Team.
3. Cochez la case correspondant au membre de l'équipe dont l'invitation est en attente.
4. Choisissez Révoquer.
5. Confirmez votre choix et choisissez Révoquer l'invitation.

Renvoyer une invitation à un membre de l'équipe dans AWS Settings

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Vous pouvez renvoyer une invitation à un membre de l'équipe pour une invitation révoquée, expirée ou refusée. Lorsque vous renvoyez une invitation, le membre de votre équipe reçoit un nouvel e-mail avec une date d'expiration 14 jours à compter de la date à laquelle vous avez renvoyé l'invitation.

Pour renvoyer une invitation

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Team.
3. Cochez la case correspondant au membre de l'équipe dont l'invitation a été révoquée, expirée ou refusée.
4. Choisissez Renvoyer.
5. Confirmez votre choix et choisissez Renvoyer l'invitation.

Mettez à jour votre compte dans AWS Settings

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Lorsque vous vous inscrivez avec Sign up for AWS (new), vos comptes sont dans la version gratuite. Dans le niveau gratuit, vous recevez un crédit d'inscription de 100 USD et gagnez jusqu'à 100$ de crédits supplémentaires. Lorsque vous êtes à court de crédits ou que vous avez un compte qui date de plus de 6 mois, vous devez passer à un forfait payant. Vous pouvez également passer à un forfait payant à tout moment. Lorsque vous passez à un forfait payant, vous avez accès aux services répertoriés dansServices AWS inclus dans le plan payant de notre nouveau AWS expérience.

Considérations relatives à la mise à niveau de votre compte

Lorsque vous passez à un forfait payant, tenez compte des points suivants :

- Vous ne pouvez pas mettre à niveau des projets individuels. Tous vos projets sont mis à niveau lorsque vous mettez à niveau votre compte.
- Lors de la mise à niveau, vous aurez accès aux services Always Free et à des offres d'essai de courte durée.
- Vous pouvez bénéficier d'autres crédits promotionnels et remises.
- Vous devez payer les frais qui dépassent le solde créditeur.
- Vous pouvez créer une limite de dépenses pour définir le montant maximum que vous paierez par mois pour un projet. Pour de plus amples informations, veuillez consulter Créez une limite de dépenses dans AWS Settings.
- Vous ne pouvez désigner aucun projet comme étant conforme à la norme HIPAA ou à la SEC.
- Votre compte ne se ferme pas lorsque les crédits sont épuisés.
- Cela ne vous permet pas de passer àInscrivez-vous pour AWS (avancé). Aucune des fonctionnalités uniquement prises en charge pour les comptes créés à l'aide de ce logiciel ne Inscrivez-vous pour AWS (avancé) sera disponible lorsque vous mettrez à niveau votre compte. Cependant, vous pouvez le faire Activer le mode avancé AWS fonctionnalités pour votre compte.
- Vous ne pouvez pas inverser le processus de mise à niveau.

Mettez à jour votre compte dans AWS Settings

Pour mettre à jour votre compte

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Facturation.
3. Choisissez Upgrade (Mise à niveau).
4. Choisissez Démarrer.
5. Ajoutez votre mode de paiement.

   En fonction de votre localisation, il se peut que vous deviez fournir certaines informations fiscales.
6. Choisissez Mettre à niveau le compte.
7. Choisissez Continuer pour retourner au bâtiment ou choisissez Définir des limites de dépenses pour définir une limite de dépenses. Pour plus d'informations sur les limites de dépenses, consultezCréez une limite de dépenses dans AWS Settings.
8. Choisissez Accéder à la console.

Votre mise à niveau est terminée.

Créez une limite de dépenses dans AWS Settings

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Qu'est-ce qu'une limite de dépenses ?

Les limites de dépenses permettent aux développeurs d'utiliser AWS en toute confiance leur capacité à fonctionner dans le cadre d'un budget prévisible et contrôlé. Utilisez une limite de dépenses pour définir le montant maximal que vous paierez par mois pour un projet. Les limites de dépenses s'appliquent au niveau du projet. Vous pouvez imposer des limites de dépenses pour certains de vos projets et avoir d'autres projets sans limites de dépenses.

Si votre utilisation dans le cadre d'un projet atteint sa limite, AWS suspendez le projet, ce qui bloque ses ressources afin que vos coûts ne dépassent pas cette limite. Les limites de dépenses sont conçues pour l'expérimentation, l'apprentissage et les charges de travail en sandbox. Ils peuvent être utilisés dans des environnements de production lorsqu'il est acceptable de suspendre brièvement vos ressources dans les cas où vos applications entraînent des coûts imprévus.

Les limites de dépenses sont visibles par toute personne ayant accès au projet, mais ne peuvent être gérées que par les propriétaires du projet. Vous devez souscrire à un forfait payant pour créer une limite de dépenses. Pour plus d'informations, consultez Mettez à jour votre compte dans AWS Settings.

Les limites de dépenses sont un type de AWS budget.

Définissez votre limite de dépenses

Votre limite de dépenses est le plafond des coûts avant impôts de votre projet, et non des frais. Lorsque vous définissez une limite de dépenses, la valeur minimale autorisée est la plus élevée des deux valeurs suivantes : 20$ ou une estimation prudente de vos dépenses probables.

Pourquoi un minimum existe : Atteindre une limite de dépenses est une expérience perturbatrice. Le minimum existe pour qu'il soit peu probable que les variations normales de votre utilisation entraînent l'atteinte de la limite de dépenses.

Comment est calculée l'estimation prudente : L'estimation est basée sur le mois d'activité cumulé depuis le début de votre activité, mais il ne s'agit pas d'une extrapolation linéaire stricte. AWS examine vos dépenses à ce jour et les ressources dont vous disposez actuellement. AWS utilise également votre activité du mois précédent ; si elle était élevée, elle devient le minimum.

Si vous avez de nombreuses ressources en cours de fonctionnement : l'estimation prudente de vos dépenses probables sera élevée. Si vous souhaitez définir une limite de dépenses inférieure, vous devez d'abord arrêter ces ressources.

Si vous réactivez un projet suspendu : l'estimation prudente de vos dépenses probables correspond à vos dépenses cumulées au cours du mois, plus toute utilisation non facturée.

> **Note**
>
> Les limites de dépenses excluent les crédits et s'appliquent aux frais avant impôts.

Notifications

Vous recevrez des notifications lorsque les coûts réels atteindront 50 %, 75 % et 90 % de votre limite, ou lorsque vous êtes sur le point d'atteindre ou de dépasser votre limite de dépenses dans les 10 prochains jours.

Personnalisez vos paramètres de limite de dépenses grâce à des contrôles anticipés des coûts optionnels

Votre limite de dépenses empêche votre facture d'augmenter au-delà du montant que vous avez fixé. Si votre consommation atteint ce seuil, AWS suspendez vos ressources pour vous protéger. Ces commandes optionnelles agissent plus tôt et plus doucement, ce qui vous permet de rester bien en deçà de la limite.

Arrêter la création de nouvelles ressources

Environ 7 jours avant que vous n'atteigniez votre limite, les nouvelles ressources cessent d'être lancées. Ceci est réalisé grâce à l'application d'une politique de contrôle des services gérée par AWS. La politique de contrôle des services dépend du service. Pour consulter toutes les politiques de contrôle des services susceptibles d'être appliquées à votre projet, voirPolitiques de contrôle des services pour les limites de dépenses.

Toutes vos ressources déjà actives continuent de fonctionner. Dans la plupart des cas, rien de ce que vous avez construit n'est affecté. Cependant, dans certains cas, cela peut entraîner une expérience perturbatrice. Par exemple, si vous avez activé l'auto-scaling et si les conditions sont réunies pour exécuter cette action, les nouvelles instances ne seront pas lancées.

Suspendre les ressources inactives

Environ 5 jours avant que vous n'atteigniez votre limite, les ressources inactives sont suspendues. Vos applications actives continuent de fonctionner. Les ressources inactives sont suspendues conformément aux recommandations de AWS Compute Optimizer. Pour plus d'informations, voir Afficher les recommandations d'inactivité.

Vous pouvez également consulter vos recommandations relatives aux ressources inutilisées en vous connectant à votre projet et en consultant les opportunités d'économies. Pour plus d'informations, consultez Cost Optimization Hub. À l'heure actuelle, dans le cadre de votre expérience en matière de limites de dépenses, nous allons automatiquement suspendre EC2, RDS et SageMaker les terminaux.

Pourquoi nous suspendons une instance EC2 : nous suspendons les instances EC2 si le pic d'utilisation du processeur est inférieur à 5 % et si votre réseau I/O est inférieur à 5 Mo par jour au cours des 14 derniers jours.

Si vous avez un type d'instance G ou P, le critère d'inactivité est différent. Les types d'instances G ou P seront suspendus si les conditions suivantes sont vraies au cours des 14 derniers jours :

- Le GPU ne fonctionne pas activement pendant plus de 99 % de la période rétrospective
- L’encodeur GPU n’est pas utilisé pendant 99 % ou plus du temps d’exécution de l’instance
- L'utilisation de la mémoire GPU au niveau de l'instance est inférieure à 5 %
- L’utilisation maximale du processeur est inférieure à 5 %
- L'utilisation du réseau est inférieure à 5 % MB/day

Pourquoi nous interrompons une base de données RDS : nous interrompons RDS pour MySQL et RDS pour PostgreSQL si l'instance de base de données n'est pas une réplique en lecture et présente les caractéristiques suivantes au cours des 14 derniers jours :

- Aucune connexion à la base de données
- Faible utilisation du processeur
- Faible read/write activité

Pourquoi nous suspendons un point de SageMaker terminaison inactif : nous SageMaker suspendons les points de terminaison si le point de terminaison n'a reçu aucun appel au cours des 14 derniers jours.

Suspendre les principaux facteurs de coûts

Environ 4 jours avant que vous n'atteigniez votre limite, vos ressources actives les plus coûteuses sont suspendues. Cela peut être une expérience perturbatrice. À l'heure actuelle, nous sélectionnons les ressources parmi ces cinq services : EC2, RDS, Lambda, Bedrock et. SageMaker Ce contrôle opt-in peut vous éviter d'encourir des frais si vous êtes confronté à un Lambda galopant ou à un pic inattendu de Bedrock.

Que se passe-t-il si vous atteignez votre limite

AWS suspend votre projet et arrête toutes les ressources. Vos données sont préservées.

Pour réactiver votre projet, augmentez votre limite de dépenses dans AWS les paramètres. Après la réactivation, certaines ressources devront peut-être être redémarrées manuellement.

> **Important**
>
> Si vous ne prenez aucune mesure dans les 90 jours suivant la suspension de votre projet, les données du projet sont AWS définitivement supprimées.

Autres points importants à noter

- Si vous utilisez Amazon Route 53, vous ne pouvez acheter qu'un seul domaine toutes les 24 heures. Vous devez vous assurer que les coûts du domaine respectent les limites de dépenses, sinon votre achat de domaine ne sera pas accepté. Dans de tels cas, vous devez augmenter les limites de dépenses avant d'effectuer un achat.
- Vous pouvez appliquer des limites de dépenses à un maximum de 10 projets.

Créez une limite de dépenses dans AWS Settings

Pour créer une limite de dépenses dans AWS Settings

1. Ouvrez AWS les paramètres sur https://settings.aws.com.
2. Dans le volet de navigation principal, sélectionnez Facturation.
3. Dans Coût par projet, pour Limite de dépenses, choisissez Définir la limite pour un projet.
4. Vous pouvez choisir la limite de dépenses recommandée ou une limite personnalisée.
5. Si vous choisissez une limite personnalisée, entrez le montant personnalisé.
6. Choisissez Définir une limite de dépenses.
7. Pour personnaliser votre limite de dépenses grâce à un contrôle précoce des coûts, vous pouvez sélectionner Arrêter le lancement de nouvelles ressources, Suspendre les ressources inutilisées ou Suspendre les principaux facteurs de coûts.
8. Choisissez Enregistrer les contrôles précoces des coûts.

La limite de dépenses entrera en vigueur immédiatement.

Mettre à jour une limite de dépenses dans AWS Settings

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Le propriétaire du projet peut mettre à jour une limite de dépenses dans AWS les paramètres à tout moment. Vous pouvez augmenter ou diminuer votre limite de dépenses, ou modifier les contrôles anticipés facultatifs des coûts. Si vous avez AWS bloqué le lancement de nouvelles ressources ou suspendu des ressources parce que vous approchez de votre limite, vous pouvez augmenter votre limite de dépenses. Si votre projet a été suspendu parce que vous avez atteint votre limite, augmentez votre limite de dépenses pour réactiver votre projet. Pour plus d'informations sur le fonctionnement des limites de dépenses, consultezCréez une limite de dépenses dans AWS Settings.

Mettre à jour une limite de dépenses dans AWS Settings

Pour mettre à jour une limite de dépenses

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Facturation.
3. Dans Coût par projet, pour Limite de dépenses, choisissez l'icône en forme de crayon.
4. Pour Limite de dépenses mensuelle (USD), entrez une nouvelle limite de dépenses.

   Nous fournissons une recommandation basée sur vos dépenses actuelles.
5. Pour modifier les protections que vous souhaitez appliquer à votre projet, sélectionnez Arrêter le lancement de nouvelles ressources, Suspendre les ressources inactives ou Suspendre les principaux facteurs de coûts.
6. Choisissez Save settings (Enregistrer les paramètres).

Les modifications de la limite de dépenses entreront en vigueur immédiatement.

Supprimer une limite de dépenses dans AWS Settings

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Le propriétaire du projet peut supprimer une limite de dépenses dans AWS les paramètres à tout moment. Lorsque vous supprimez une limite de dépenses, AWS vous ne contrôlez plus vos coûts et ne contrôlez plus les coûts de votre projet à un stade précoce. Pour plus d'informations sur le fonctionnement des limites de dépenses, consultezCréez une limite de dépenses dans AWS Settings.

Supprimer une limite de dépenses dans AWS Settings

Pour supprimer une limite de dépenses

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Facturation.
3. Dans Coût par projet, pour Limite de dépenses, choisissez l'icône en forme de crayon.
4. Choisissez Supprimer la limite.
5. Confirmez votre choix et choisissez Supprimer.

Votre limite de dépenses sera supprimée immédiatement.

Niveau gratuit dans notre nouveau AWS expérience

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Vous pouvez utiliser le niveau AWS gratuit pour explorer les AWS services sans engagement financier. Si vous êtes nouveau AWS, vous recevez 100 USD de crédits après avoir créé un compte, quel que soit votre plan de compte. Vous pouvez également gagner jusqu'à 100 USD

supplémentaires sur l'ensemble de vos projets sous forme de crédits en effectuant des activités. Pour plus d'informations sur l'obtention de crédits supplémentaires, consultezGagnez des crédits supplémentaires. De plus, vous avez accès à plus de 30 AWS services toujours gratuits qui offrent des limites d'utilisation gratuites mensuelles.

Le plan de compte gratuit est idéal pour les clients qui expérimentent des AWS services et élaborent des preuves de concept gratuitement pendant une période maximale de six mois. Aucuns frais ne vous seront facturés pendant cette période jusqu'à ce que vous passiez à un forfait de compte payant. Votre forfait de compte gratuit prend fin au bout de six mois ou lorsque vos crédits sont entièrement utilisés, selon la première éventualité. De plus, les plans de compte gratuits ne donnent pas accès à certains AWS services qui consommeraient rapidement la totalité du montant du crédit du niveau AWS gratuit ou des achats de matériel. Pour obtenir la liste des services éligibles inclus dans le plan de compte gratuit, consultez la section AWS Services pris en charge pour l'inscription AWS (nouveau).

Le plan de compte payant est idéal pour créer des applications de production qui vont au-delà du montant du crédit initial. Lorsque votre utilisation dépasse votre solde créditeur ou lorsque vous utilisez un service où les crédits ne s'appliquent pas, vous payez le tarif standard de paiement à l'utilisation.

Tous les projets que vous possédez sont régis par le même type de plan. Si vous passez au plan de compte payant, tous vos projets ont accès à des services supplémentaires, et vous payez le tarif standard de paiement à l'utilisation pour tous les projets. Pour plus d'informations, consultez la section Mettre à niveau votre compte dans AWS les paramètres.

Vous pouvez utiliser la console de gestion des coûts pour suivre votre utilisation de tous les AWS services proposant un niveau gratuit pour votre projet.

Suivi de votre utilisation de l'offre gratuite

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

AWS Les alertes d'utilisation du niveau gratuit vous avertissent automatiquement par e-mail lorsque vous dépassez 85 % de votre limite de niveau gratuit pour chaque service. Pour un suivi supplémentaire, vous pouvez configurer le suivi de votre utilisation jusqu'à 100 % de la limite du

niveau gratuit en définissant un budget de dépenses nul. Vous pouvez également filtrer votre budget pour suivre des services individuels.

Vous pouvez suivre votre utilisation du niveau AWS gratuit de la manière suivante.

Utilisation AWS Settings

Vous pouvez surveiller la date d'expiration de votre plan de compte gratuit, votre solde créditeur et les jours restants dans AWS les paramètres. Pour de plus amples informations, veuillez consulter Consultez et échangez des crédits dans AWS Settings. Vous recevez également des alertes périodiques par e-mail concernant votre solde créditeur et la date à laquelle vous approchez de la fin de la période de votre plan de compte gratuit.

Si vous avez un forfait payant, vous pouvez surveiller votre solde créditeur et sa date d'expiration sur la page des crédits dans AWS les paramètres. Pour plus d'informations sur la mise à niveau vers un forfait payant, consultezMettez à jour votre compte dans AWS Settings.

Utilisation de la console de gestion de la facturation et des coûts

Vous pouvez utiliser la console de gestion de la facturation et des coûts pour suivre l'utilisation de votre niveau gratuit pour chaque projet. La console de gestion de la facturation et des coûts affiche un résumé de votre utilisation mensuelle et de toutes les offres de services supérieures ou égales aux limites d'utilisation. Pour chaque offre de niveau gratuit en cours d'utilisation, vous pouvez consulter les informations suivantes :

- Le service
- La limite d'utilisation du niveau AWS gratuit
- Votre utilisation actuelle
- Votre consommation prévue
- Votre consommation réelle depuis le début du mois (MTD)
- Votre consommation mensuelle prévue (MTD)

La procédure suivante vous montre comment utiliser la console de gestion de la facturation et des coûts pour trier votre utilisation du niveau gratuit en fonction de votre utilisation mensuelle réelle.

Pour trier votre utilisation du niveau gratuit

1. Ouvrez la console Billing and Cost Management à l'adresse https://console.aws.amazon.com/cost-management/.

2. Choisissez le niveau gratuit.
3. Pour trier par utilisation réelle depuis le début du mois, choisissez % d'utilisation réelle MTD.

Gagnez des crédits supplémentaires

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Si vous êtes un nouveau AWS client, vous pouvez gagner 100 USD supplémentaires en crédits, quel que soit votre plan de compte, en effectuant des activités. Ces activités vous aident à vous familiariser avec les AWS services. Vous pouvez trouver les activités dans le AWS widget Explore sur le tableau de bord de votre AWS console d'accueil. Toutes ces activités entraîneront des frais de AWS service qui seront déduits de vos crédits de niveau AWS gratuit, mais lorsque vous terminez chaque activité, vous recevez 20 USD de crédits.

Activités à réaliser

- Lancer une instance à l'aide d'Amazon EC2
- Utilisez un modèle fondamental dans le terrain de jeu Amazon Bedrock
- Créez un budget
- Création d'une application Web à l'aide de Lambda
- Création d'une base de données Amazon RDS

Consultez vos informations de facturation dans AWS Settings

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Vous pouvez utiliser AWS les paramètres pour consulter vos informations de facturation. Si vous utilisez le niveau gratuit, cette page vous indique le nombre de jours dont vous disposez et vos AWS

crédits. Vous pouvez également consulter le coût par projet. Si vous utilisez le forfait payant, vous pouvez consulter votre solde, les frais actuels et le coût par projet. Si vous utilisez une limite de dépenses, vous pouvez consulter les informations relatives à votre limite. Vous pouvez également Gérez votre mode de paiement dans AWS Settings etGérez l'enregistrement fiscal dans AWS Settings.

Lorsque vous utilisez le plan gratuit, toute utilisation est couverte par vos crédits du niveau AWS gratuit. Vous devez passer au forfait payant si vous épuisez vos crédits de niveau AWS gratuit ou après 184 jours, selon la première éventualité. Pour plus d'informations sur la mise à niveau vers un forfait payant, consultezMettez à jour votre compte dans AWS Settings.

Pour consulter vos coûts par projet

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Facturation.
3. Sous Coût par projet, vous verrez vos frais mensuels et les frais mensuels prévus. Vous verrez tous les frais relatifs à vos projets.
4. (Facultatif) Pour afficher une ventilation de vos frais pour un projet dans la section Inspecter les coûts, choisissez Afficher. Vous serez redirigé vers la console de gestion AWS de la facturation et des coûts.

Vos données de facturation et les données Cost Explorer que vous voyez sur la console de gestion AWS de la facturation et des coûts sont actualisées au moins une fois par jour. La cadence à laquelle ils sont actualisés peut être différente. Si vous utilisez une limite de dépenses, cela peut entraîner des différences quant à vos frais estimés depuis le début du mois dans les AWS paramètres et la console de gestion des AWS coûts.

Consultez votre historique de facturation dans AWS Settings

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Vous pouvez consulter votre historique de facturation dans AWS les paramètres. Votre historique de facturation n'est disponible que si vous disposez d'un mode de paiement. Si vous utilisez le niveau gratuit, vous ne verrez pas votre historique de facturation.

Vous pouvez télécharger les factures de chaque fournisseur de services avec lequel vous avez effectué des transactions au cours de la période de facturation. Cela inclut des informations telles que le type de frais, la date de facturation et le total en dollars américains. Si vos factures sont émises dans une autre devise, le total dans cette autre devise est également indiqué. Les factures ne sont pas réparties entre chaque projet.

Pour consulter votre historique de facturation

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Facturation.
3. À côté de Solde, choisissez Afficher l'historique de facturation. Vous serez redirigé vers l'historique de facturation.
4. Pour télécharger une facture, sélectionnez un numéro de facture.

Gérez votre mode de paiement dans AWS Settings

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Vous pouvez gérer votre mode de paiement dans AWS les paramètres. Votre mode de paiement est utilisé pour payer l'utilisation AWS des ressources dans tous vos projets. Vous ne pouvez gérer votre mode de paiement que si vous avez fourni des informations lors de la création de votre compte ou si vous avez fait passer votre compte au forfait payant.

Pour gérer votre mode de paiement

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Facturation.
3. Sous Solde, vous verrez vos informations de paiement. Choisissez Gérer.
4. Pour Mode de paiement, choisissez Mettre à jour.

5. Entrez votre nouveau mode de paiement et choisissez Enregistrer.

Effectuez un paiement en AWS Settings

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Vous pouvez payer votre AWS facture dans AWS les paramètres. AWS débite automatiquement votre mode de paiement par défaut au début de chaque mois. En cas d'échec du débit, vous pouvez utiliser la console pour mettre à jour votre moyen de paiement et procéder au paiement.

Avant d'effectuer un paiement, assurez-vous que le mode de paiement que vous souhaitez débiter automatiquement à l'avenir est défini comme mode de paiement par défaut. Si vous utilisez une carte de crédit, confirmez qu'elle n'a pas expiré.

Pour effectuer un paiement

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Facturation.
3. À côté de Solde, choisissez Afficher l'historique de facturation. Vous serez redirigé vers l'historique de facturation.
4. Sous Action, vous verrez Payer la facture pour toute facture impayée. Si aucune facture n'est répertoriée, vous n'avez rien à faire.
5. Choisissez Payer la facture.
6. Confirmez votre choix et choisissez Payer.

Si vous avez des questions concernant les problèmes liés au débit de votre compte bancaire ou au règlement du solde après échéance, créez une demande dans le Centre de support.

Changez votre devise préférée en AWS Settings

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Vous pouvez modifier la devise de votre choix dans AWS les paramètres. Votre devise préférée ne s'applique qu'aux projets dont vous êtes propriétaire. Certains pays de facturation limitent les devises de paiement. L'émetteur de votre carte peut facturer des frais pour les transitions dans d'autres devises.

Pour modifier votre devise d'affichage préférée

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Facturation.
3. Sous Solde, vous verrez vos informations de paiement. Choisissez Gérer. Si vous ne voyez pas de solde, vous ne pouvez pas changer la devise.
4. Choisissez Définir la devise.
5. Pour Devise de paiement par défaut, sélectionnez la devise de paiement.
6. Choisissez Enregistrer.

Gérez l'enregistrement fiscal dans AWS Settings

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Vous gérez vos numéros d'immatriculation fiscale et vos exonérations fiscales dans AWS les paramètres. Vos informations fiscales ne s'appliquent qu'aux projets dont vous êtes propriétaire.

Mise à jour et suppression de numéros d'enregistrement fiscal

Suivez les étapes suivantes pour mettre à jour ou supprimer un ou plusieurs numéros d'enregistrement fiscal.

> **Note**
>
> Si un pays ne figure pas dans la liste déroulante de la page des paramètres fiscaux, l'enregistrement fiscal de ce pays AWS n'est pas collecté pour le moment.

Pour mettre à jour les numéros d'enregistrement fiscal

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Facturation.
3. Sous Solde, vous verrez vos informations de paiement. Choisissez Gérer.
4. Choisissez Paramètres fiscaux.
5. Modifiez vos informations d'enregistrement fiscal.
6. Choisissez Enregistrer.

Gestion de vos exonérations fiscales américaines

Si votre État est éligible, vous pouvez gérer vos exonérations fiscales américaines sur la page Plan et facturation dans AWS les paramètres. Les documents que vous téléchargez pour bénéficier de l'exemption sont examinés par le support dans les 24 heures. Vous ne pouvez gérer vos exonérations fiscales que si votre compte est enregistré en tant qu'entreprise.

Pour charger ou ajouter votre exonération fiscale américaine

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Facturation.
3. Sous Solde, vous verrez vos informations de paiement. Choisissez Gérer.
4. Choisissez Manage tax exemption (Gérer une exonération fiscale) et sélectionnez Add tax exemption (Ajouter une exonération fiscale).
5. Spécifiez votre type d'exonération et votre juridiction.

6. Chargez des documents de certificat.
7. Vérifiez les informations que vous avez saisies, puis choisissez sur Submit (Envoyer).

Dans les 24 heures, le support vous informera par le biais d'un dossier d'assistance s'il a besoin d'informations supplémentaires ou si l'un de vos documents n'était pas valide.

Une fois l'exonération approuvée, vous la trouverez sous l'onglet Exonération fiscale avec une période de validité Actif.

Si votre exonération a été rejetée, vous en serez informé par le biais d'un contact de support.

Consultez et échangez des crédits dans AWS Settings

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Vous pouvez consulter et utiliser vos crédits disponibles dans AWS les paramètres. AWS les crédits sont automatiquement appliqués aux factures pour aider à couvrir les coûts associés aux services éligibles. Pour plus d'informations sur les services éligibles, consultez Utiliser votre crédit AWS promotionnel. Les crédits sont appliqués à tous les projets que vous possédez jusqu'à leur épuisement ou leur expiration. Vous ne pouvez pas sélectionner le projet qui utilise les crédits que vous échangez, ils sont appliqués à tous les projets que vous possédez.

Pour consulter vos crédits

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Facturation.
3. Dans le conteneur Frais courants, vous verrez vos crédits disponibles. Choisissez vos crédits.

   Vous serez redirigé vers la liste des crédits actifs et expirés, ou vers la liste de vos crédits et des crédits inactifs des 6 derniers mois, selon le type de forfait.
4. Pour voir les AWS services qui peuvent être utilisés avec vos crédits, choisissez Voir la liste des services.

Pour échanger votre AWS Crédits promotionnels

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Facturation.
3. Dans le conteneur Frais courants, vous verrez vos crédits disponibles. Choisissez vos crédits.

   Vous serez redirigé vers la liste des crédits actifs et expirés, ou vers la liste de vos crédits et des crédits inactifs des 6 derniers mois, selon le type de forfait.
4. Choisissez Utiliser le crédit pour échanger vos crédits.
5. Pour le code promotionnel, entrez le code promotionnel tel qu'il apparaît. Lorsque vous utilisez le crédit, vous indiquez que vous avez lu et accepté les conditions générales des crédits AWS promotionnels.
6. Choisissez Utiliser le crédit.

Gérez des comptes en Inde dans AWS Settings

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Si vous vous inscrivez 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).

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).

Rubriques

- Inscrivez-vous pour AWS (nouveau) avec AWS Inde
- Gérez les informations de vérification de vos clients

Inscrivez-vous pour AWS (nouveau) avec AWS Inde

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

Pour utiliser Inscrivez-vous pour AWS (nouveau) avec AWS Inde

1. Accédez à aws.amazon.com et choisissez Créer un compte.
2. Sur la bannière expliquant les différences entre S'inscrire pour AWS (nouveau) et S'inscrire pour AWS (avancé), choisissez S'inscrire pour AWS.
3. Choisissez un identifiant tel que Google GitHub, Apple ou Amazon.
4. Vous serez redirigé vers l'identifiant de votre fournisseur. Une fois connecté, vous serez redirigé pour vous AWS inscrire.
5. Entrez votre nom et choisissez Continuer.

   Ce nom sera communiqué aux membres de l'équipe lorsque vous leur donnerez accès à vos projets.
6. Vérifiez l'e-mail associé à votre identifiant en saisissant un code de vérification. Lorsque vous avez vérifié votre adresse e-mail, choisissez Continuer.
7. Entrez un mot de passe sécurisé pour votre compte et 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
   - Il doit inclure au moins trois des types de caractères suivants : majuscules, minuscules, chiffres et ! @ # $ % ^ portail de gestion * () <> [] {} | _+-= symboles.
   - Il ne doit pas être identique à votre Compte AWS nom ou à votre adresse e-mail.
8. Entrez vos coordonnées et choisissez Continuer.

   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".

9. Choisissez l'objectif principal de l'enregistrement de votre compte.
10. 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.
11. 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.

12. 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.
13. 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 profil dans Mes AWS paramètres. Vous devez passer la vérification client pour accéder aux AWS services.
14. AWS fournira votre premier projet.

Pour accéder aux AWS paramètres, choisissez Gérer les projets dans le Console de gestion AWS. Dans AWS Paramètres, vous pouvez inviter des membres de l'équipe, créer de nouveaux projets et modifier vos paramètres de facturation et autres.

Gérez les informations de vérification de vos clients

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 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 de facturation, votre adresse et d'autres informations de contact, consultezUtilisation AWS Settings. Si vous modifiez des informations que vous avez précédemment utilisées pour la vérification des clients, telles que le nom ou l' India-based adresse 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 Gérer le profil. 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. Ouvrez AWS les paramètres sur https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Gérer le profil.
3. Pour la vérification du client, choisissez Créer une vérification du 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 Soumettre.

   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. Ouvrez AWS les paramètres sur https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Gérer le profil.
3. Pour la vérification du client, 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 Soumettre.

   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.
- Identification de l'électeur Card/EPIC - La carte d'identité de l'électeur, également connue sous le nom de carte d'identité avec photo des électeurs (EPIC), contient un numéro d'identification unique délivré par la Commission électorale de l'Inde aux électeurs éligibles en Inde. Un ID/EPIC numéro 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.

- 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' card/EPICélecteur et permis de conduire.
- Pour les comptes professionnels - carte PAN et certificat de constitution.

Configurez votre facturation en Inde dans AWS Settings

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Si vous vous inscrivez 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 AWS vendeur local en Inde. AWS L'Inde gère votre facturation et le total de votre facture est indiqué en roupies au lieu de dollars. Toutes les informations fiscales ne peuvent être créées ou modifiées que par le propriétaire du projet.

Pour obtenir des informations fiscales ou de facturation supplémentaires, vous pouvez utiliser la AWS Billing console pour chaque projet.

Utilisez la section Forfait et facturation de la page Gérer le profil des AWS paramètres pour effectuer les tâches suivantes :

- Ajouter ou modifier un numéro PAN (Permanent Account Number, numéro de compte permanent)

- Modifier plusieurs numéros PAN (Permanent Account Number, numéros de comptes permanents)
- Modifier plusieurs numéros de taxe sur les biens et services (GST)
- Afficher une facture fiscale

Ajouter ou modifier un numéro PAN (Permanent Account Number, numéro de compte permanent)

Vous pouvez ajouter votre numéro PAN (Permanent Account Number, numéro de compte permanent) à votre compte et le modifier.

Pour ajouter ou modifier un numéro PAN

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Gérer le profil, puis choisissez Forfait et facturation.
3. Dans la barre de navigation Paramètres des taxes, choisissez Modifier.
4. Pour Numéro PAN (Permanent Account Number, numéro de compte permanent), saisissez votre numéro PAN, puis choisissez Mettre à jour.

Modifier plusieurs numéros PAN (Permanent Account Number, numéros de comptes permanents)

Vous pouvez modifier plusieurs numéros de compte permanent (PAN) dans votre compte.

Pour modifier plusieurs numéros PAN

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Gérer le profil, puis choisissez Forfait et facturation.
3. Sous Manage Tax Registration Numbers (Gérer les numéros d'enregistrement fiscal), sélectionnez les numéros PAN que vous souhaitez modifier.
4. Pour Manage Tax Registration (Gérer l'enregistrement fiscal), choisissez Edit (Modifier).
5. Mettez à jour les champs que vous souhaitez modifier, puis choisissez Update (Mettre à jour).

Modifier plusieurs numéros de taxe sur les biens et services (GST)

Vous pouvez modifier plusieurs numéros de taxe australienne sur les biens et services (GST) dans votre compte.

Pour modifier plusieurs numéros GST

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Gérer le profil, puis choisissez Forfait et facturation.
3. Sous Manage Tax Registration Numbers (Gérer les numéros d'enregistrement fiscal), sélectionnez les numéros GST que vous souhaitez modifier ou choisissez Edit all (Modifier tout).
4. Pour Manage Tax Registration (Gérer l'enregistrement fiscal), choisissez Edit (Modifier).
5. Mettez à jour les champs que vous souhaitez modifier et choisissez Update (Mettre à jour).

Afficher une facture fiscale

Vous pouvez consulter vos factures fiscales dans AWS les paramètres.

Pour consulter une facture fiscale

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Gérer le profil, puis choisissez Forfait et facturation.
3. Faites défiler vers le bas et choisissez l'onglet Invoices (Factures).
4. Dans la section Factures fiscales, choisissez un lien de facture mentionné sous Numéro du document.

> **Note**
>
> La section Tax invoices (Factures fiscales) n'apparaît que si des factures fiscales sont disponibles.

Changer le vendeur enregistré vers ou depuis AWS Inde

Vous pouvez remplacer votre Compte AWS vendeur enregistré (SOR) par un autre SOR en mettant à jour vos informations de facturation ou fiscales. Cela ne s'applique pas si votre compte AWS indien fonctionne selon le modèle existant où la fonctionnalité n'est pas disponible. Lorsque vous modifiez votre pays ou votre région dans vos informations de facturation ou fiscales, le SOR de votre compte change automatiquement si le fournisseur de services de la nouvelle localisation est différent de votre position actuelle.

Si vous modifiez votre compte à destination ou AWS en provenance de l'Inde, vous n'avez pas besoin de mettre à jour votre mode de paiement par défaut s'il est configuré sur facture ou virement bancaire. Si votre mode de paiement par défaut est une carte de crédit ou de débit, vous devez reconfirmer les informations de votre carte de paiement par défaut. Cela permet de garantir que le mode de paiement est stocké séparément des transactions en dehors de l' AWS Inde. Pour plus d'informations, voir Consulter les cartes de crédit ou de débit éligibles pour les factures AWS en Inde.

> **Note**
>
> Si vous possédez un compte AWS en Inde avec une carte de crédit ou de débit comme mode de paiement par défaut et que le mandat électronique est configuré pour les paiements automatiques, vous devez désactiver le mandat électronique avant de pouvoir modifier vos préférences de paiement par défaut.

Pour modifier le SOR de votre compte, vous pouvez modifier ces informations à l'aide des options suivantes :

Pour modifier le SOR à l'aide des informations de facturation et fiscales

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Gérer le profil, puis choisissez Forfait et facturation.
3. Dans la section Préférences de paiement par défaut, choisissez Modifier.
4. Entrez la nouvelle adresse de facturation.
5. Dans la section Devise de paiement, choisissez une devise par défaut dans la liste des devises acceptées de votre nouveau SOR.

6. (Si votre mode de paiement par défaut est une carte de crédit ou de débit) Dans la section Confirmer le mode de paiement, saisissez à nouveau les informations de votre carte de paiement par défaut pour confirmer son utilisation auprès du nouveau fournisseur de services.

   Pour modifier les cartes par défaut dans le cadre du nouveau SOR, ajoutez votre carte ultérieurement et modifiez les paramètres de votre mode de paiement par défaut.

7. Sélectionnez Enregistrer les modifications.

   Après quelques minutes, vos modifications, y compris le SOR mis à jour, apparaissent sur la page des préférences de paiement.

Pour modifier le SOR à l'aide des informations de facturation et fiscales

Pour transférer votre compte vers un autre SOR, vous devez mettre à jour le numéro d'enregistrement fiscal (TRN) associé au compte et fournir un nouveau TRN valide. Vous pouvez également supprimer le TRN associé au compte. Le nouveau SOR de votre compte est automatiquement résolu en fonction du pays de votre nouvelle adresse fiscale et de votre adresse de facturation actuelle, par ordre de disponibilité et de priorité. Lorsque le SOR de votre compte change, vous recevez une notification indiquant que votre compte est transféré vers ou hors de AWS l'Inde.

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Gérer le profil, puis choisissez Forfait et facturation.
3. Sélectionnez votre compte et choisissez Gérer l'enregistrement fiscal, puis choisissez Modifier , Tout modifier ou Supprimer le TRN.
4. (Si votre mode de paiement par défaut est une carte de crédit ou de débit) Dans le volet de navigation principal, choisissez Gérer le profil, puis choisissez Forfait et facturation.
5. Choisissez Ajouter un mode de paiement pour saisir à nouveau les informations de votre carte de paiement par défaut, ou ajoutez une nouvelle carte de paiement.
6. Une fois la carte enregistrée, choisissez Définir par défaut.

   La section Préférences de paiement par défaut vous indique que votre ancien mode de paiement par défaut ne peut pas être utilisé dans le nouveau SOR. Actualisez la page après avoir ajouté votre carte de paiement pour que cette alerte disparaisse.

Accès AWS Support

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Lorsque vous vous inscrivez à notre nouvelle AWS expérience, vous pouvez travailler avec le AWS Support à deux endroits.

Vous pouvez accéder à Basic Support ou Business Support+. Par défaut, vous êtes inscrit au Support de base. Vous pouvez commencer un essai de Business Support+ pour l'utiliser gratuitement pendant six mois au maximum.

Accompagnement de projets

Si vous rencontrez des problèmes liés à votre projet, à la gestion de votre équipe ou à la facturation, vous pouvez accéder à Basic Support ou Business Support+ dans AWS les paramètres. Vous pouvez demander des projets supplémentaires pour votre organisation ou demander des augmentations de quotas liées à la facturation.

Pour créer une demande de support

1. Ouvrez AWS les paramètres sur https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Support.
3. Pour le support du projet, choisissez Créer un dossier.
4. Dans le champ Objet, saisissez l'objet de votre demande d'assistance.
5. Dans le champ Description, décrivez votre problème. Si possible, décrivez les étapes à suivre pour reproduire le problème.
6. Choisissez Create case (Créer une demande).

Après avoir créé un dossier d'assistance, vous pouvez consulter les informations relatives à votre dossier pour continuer à travailler avec le support.

Pour consulter les informations relatives à votre dossier

1. Ouvrez AWS les paramètres sur https://settings.aws.com.

2. Dans le volet de navigation principal, choisissez Support.
3. Sélectionnez votre cas de support. Dans cette vue, vous pouvez voir toutes les communications relatives à votre dossier.
4. Pour envoyer une réponse au support, dans Répondre, saisissez votre réponse, puis choisissez Envoyer la réponse.

Lorsque votre cas est résolu, vous pouvez le résoudre pour le supprimer des AWS paramètres.

Pour résoudre votre cas

1. Ouvrez AWS les paramètres sur https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Support.
3. Choisissez Resolve case (Résoudre le cas).

Vous ne pourrez pas accéder aux détails du dossier une fois celui-ci résolu.

Support technique

Si vous rencontrez des problèmes avec vos AWS ressources, vous avez besoin d'une assistance technique. Pour accéder au support technique, ouvrez un dossier dans le Centre de AWS support pour le projet concerné.

Support si tous vos projets et votre organisation sont fermés

Si tous vos projets et votre organisation sont fermés, contactez le support en remplissant le formulaire de commentaires sur le support.

Dans la section Demande d'informations, sous Comment pouvons-nous vous aider, indiquez que vous utilisez notre nouvelle AWS expérience et que tous vos projets sont clôturés.

Démarrez un essai Business Support+

Vous pouvez bénéficier de Business Support+ gratuitement pendant une période maximale de six mois. Business Support+ est fourni gratuitement jusqu'au 31 octobre 2026. À compter du 1er novembre 2026, la tarification standard commence et vous recevrez 174$ en crédits Business Support+ pour couvrir jusqu'à six mois de 29 dollars américains par mois. Vous restez abonné lorsque la période gratuite se termine et que les crédits commencent, et vous vous AWS avertissez lorsque votre solde créditeur est faible avant le début de toute facturation au tarif complet.

Vos frais Business Support+ sont de $ 29/month ou d'un pourcentage de vos AWS dépenses, selon le montant le plus élevé. Pour plus d'informations, consultez le détail des tarifs. Votre forfait est renouvelé tous les mois jusqu'à ce que vous le résiliiez.

Pour démarrer votre essai Business Support+

1. Ouvrez AWS les paramètres sur https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Support.
3. Choisissez Commencer l'essai. Cela aura une incidence sur tous les projets de votre organisation.
4. Passez en revue les conditions, cochez la case du contrat, puis choisissez Commencer l'essai.

Vous pouvez annuler à tout moment sans engagement ni pénalité. Lorsque vous annulez, l'accès à Business Support+ prend fin immédiatement et tous les crédits non utilisés sont perdus. Vous pouvez vous réinscrire au tarif standard à tout moment, mais l'offre promotionnelle Business Support+ ne peut pas être rétablie une fois annulée.

Pour annuler Business Support+

1. Ouvrez AWS les paramètres sur https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Support.
3. Choisissez Annuler le plan.
4. Cochez cette case pour confirmer que l'annulation de Business Support+ vous permet de revenir immédiatement au support de base, que vous perdrez l'accès aux avantages listés et que vos 174$ de crédits seront supprimés et ne pourront pas être rétablis.
5. Choisissez Annuler le plan pour revenir au Support de base.

Surveillez votre projet à l'aide de AWS CloudTrail

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Surveillez votre projet à l'aide de AWS CloudTrail

Votre projet est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un membre de l'équipe ou un AWS service. CloudTrail capture tous les appels d'API pour votre projet sous forme d'événements. Les appels capturés incluent les appels provenant de la console et les opérations d'API pour tous les AWS services pris en charge. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à votre projet, la personne qui l'a faite, la date à laquelle elle a été faite et des informations supplémentaires.

CloudTrail À utiliser pour voir qui a modifié votre projet

Ce didacticiel est destiné aux utilisateurs qui sont à l'aise avec le AWS CLI. Si vous partagez votre projet avec plusieurs membres de l'équipe, vous pouvez l'utiliser CloudTrail pour voir qui a modifié les ressources de votre projet. Chaque action entreprise par vous ou par les membres de l'équipe lorsqu'ils utilisent AWS les paramètres ou Console de gestion AWS pour accéder à votre projet est enregistrée par le `onBehalfOf` paramètre. Ce paramètre indique un ID utilisateur et un ID de banque d'identités. Ensemble, ces valeurs définissent un identifiant de constructeur que vous avez invité à accéder à votre projet.

Pour trouver le `onBehalfOf` paramètre et le connecter à un membre de l'équipe, vous devez accéder au AWS CLI et au Console de gestion AWS. Si vous ne l'avez pas AWS CLI configuré, vous pouvez l'utiliser AWS CloudShell pour accéder à un shell pré-authentifié basé sur un navigateur que vous pouvez lancer directement depuis et exécuter des Console de gestion AWS commandes. AWS CLI

Étape 1. Pour trouver un AWS CloudTrail Événement

1. Connectez-vous à la CloudTrail console Console de gestion AWS et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, choisissez Event history (Historique des événements). Vous voyez une liste filtrée des événements, avec les événements les plus récents affichés d'abord. Choisissez un événement.
3. Dans le compte rendu de l'événement, vous verrez le contenu suivant :

```
"onBehalfOf": {
            "userId": "00000-e00f-000-000-0000000",
            "identityStoreArn":
 "arn:aws:identitystore::111122223333:identitystore/000000-0000-0000-0000-60000007"
```

```
}
```

Il s'agit de l'identité qui définit le membre de l'équipe qui a créé l' CloudTrailévénement.

Étape 2. Pour connecter le BehalfOf paramètre on à un membre de l'équipe

Pour connecter le `onBehalfOf` paramètre à un membre de l'équipe à l'aide de AWS CLI :

Pour utiliser le plugin AWS CLI dans votre terminal

1. Exécutez la commande suivante pour vous connecter au AWS CLI. Vous pouvez trouver votre région en utilisantRégions AWS pour vos projets.

   ```
   aws login --region project-region
   ```

2. Exécutez la commande suivante pour obtenir l'identifiant de votre magasin d'identités. L' CloudTrailévénement affiche l'ARN de la banque d'identités, mais n'indique pas l'ID de la banque d'identités. Vous utilisez toujours le Région AWS `us-east-1` lorsque vous recherchez l'identifiant de votre magasin d'identités.

   ```
   aws sso-admin list-instances --region us-east-1
   ```

   Le résultat se présente comme suit :

   ```
   {
       "Instances": [
           {
               "InstanceArn": "arn:aws:sso:::instance/ssoins-0000000000",
               "IdentityStoreId": "d-000000",
               "OwnerAccountId": "111122223333",
               "CreatedDate": "2025-10-26T23:10:58.529000+00:00",
               "Status": "ACTIVE",
               "PrimaryRegion": "us-east-1",
               "Regions": [
                   {
                       "RegionName": "us-east-1",
                       "Status": "ACTIVE",
                       "AddedDate": "2025-10-26T23:10:58.529000+00:00",
                       "IsPrimaryRegion": true
                   }
   ```

```
            ]
        }
    ]
}
```

Vous souhaitez copier l'identifiant de la banque d'identités. Dans ce cas, l'identifiant du magasin d'identités est `d-000000`.

3. Exécutez la commande suivante pour décrire le membre de l'équipe qui correspond au `onBehalfOf` paramètre.

```
aws identitystore describe-user --user-id 00000-e00f-000-000-0000000 --region us-
east-1 --identity-store-id d-000000
```

Le résultat se présente comme suit :

```
{
    "IdentityStoreId": "d-000000",
    "UserId": "00000-e00f-000-000-0000000",
    "UserName": "carlos_salazar",
    "Name": {
        "FamilyName": "Salazar",
        "GivenName": "Carlos"
    },
    "DisplayName": "Carlos",
    "Emails": [
        {
            "Value": "carlos_salazar@example.com",
            "Type": "work",
            "Primary": true
        }
    ],
    "UserStatus": "ENABLED",
    "CreatedAt": "2025-10-26T23:15:27.213000+00:00",
    "CreatedBy": "00000000000",
    "UpdatedAt": "2025-10-26T23:18:55.432000+00:00",
    "UpdatedBy": "0000000000"
}
```

Le nom d'affichage et les e-mails du membre de votre équipe sont fournis dans cette sortie.

Pour connecter le `onBehalfOf` paramètre à un membre de l'équipe en utilisant AWS CloudShell, connectez-vous au Console de gestion AWS and access CloudShell. Pour plus d'informations, consultez Getting started with AWS CloudShell. Vous disposerez automatiquement des autorisations IAM appropriées pour y accéder CloudShell.

Fermer un projet dans AWS Settings

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Si vous n'avez plus besoin de votre projet, vous pouvez le fermer. Une fois que vous avez fermé votre projet, vous pouvez le rouvrir dans les 90 jours suivant sa fermeture. La période qui s'écoule entre le jour où vous avez clôturé le projet et la date de sa fermeture AWS définitive correspond à la période qui suit la clôture.

Ce que vous devez savoir avant de clôturer votre projet

Avant de clôturer votre projet, tenez compte des points suivants :

- Vous ne pouvez pas fermer votre projet s'il est suspendu en raison d'un dépassement d'une limite de dépenses. Vous devez désactiver les limites de dépenses, puis clôturer le projet. Pour de plus amples informations, veuillez consulter Mettre à jour une limite de dépenses dans AWS Settings.
- Tous les membres de l'équipe perdront automatiquement l'accès à ce projet et à toutes les ressources qu'il contient.
- La clôture de votre projet constituera votre avis de résiliation du contrat AWS client pour ce projet.
- Il n'est pas nécessaire de supprimer des ressources de votre projet avant de le fermer. Nous vous recommandons toutefois de sauvegarder toutes les ressources ou données que vous souhaitez conserver. Pour obtenir des instructions sur la sauvegarde d'une ressource particulière, consultez la AWS documentation appropriée pour ce service.
- Vous pouvez rouvrir votre projet après la fermeture. Les frais pour les services restés dans votre projet reprendront si vous le rouvrez. Vous restez également responsable de toute facture impayée.
- Vous restez responsable de tous les frais et charges impayés pour les services consommés avant la clôture du projet. Vous recevrez une AWS facture le mois suivant la clôture de votre projet. 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.

- Après la clôture d'un projet, nous AWS enverrons des e-mails quotidiens pendant cinq jours maximum avant que nous ne suspendions le domaine. Une fois le domaine suspendu, 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. Ces informations sont écrites pour les projets Comptes AWS, mais elles sont exactes.
- AWS CloudTrail est un service de sécurité fondamental. Cela signifie que les pistes créées par les utilisateurs peuvent continuer d'exister et proposer des événements même après la fermeture d'un projet, à moins qu'un utilisateur ne supprime explicitement les pistes de son projet avant de le fermer. Pour plus d'informations sur la procédure à suivre pour demander la suppression d'une Compte AWS piste après la fermeture d'une piste, consultez la section Compte AWS Fermeture et pistes dans le Guide de CloudTrail l'utilisateur. Ces informations sont écrites pour les projets Comptes AWS, mais elles sont exactes.

Pour clôturer un projet

Pour clôturer un projet

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez le projet auquel vous souhaitez accéder.
3. Pour Fermer le projet, choisissez Fermer le projet.
4. Confirmez votre choix et choisissez Fermer le projet.

La page du projet affichera toujours votre projet pendant 90 jours, jusqu'à ce qu'il soit définitivement supprimé.

Post-closure période

La période postérieure à la clôture fait référence à la période qui s'écoule entre le jour où vous avez fermé votre compte et la date de fermeture AWS définitive de votre projet. La période suivant la fermeture est de 90 jours. Après la fermeture, vous ne pourrez accéder à votre contenu et à vos AWS services qu'en rouvrant votre projet. Après la période de clôture, ferme AWS définitivement votre projet 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 projet, son identifiant de projet ne peut jamais être réutilisé.

Réouverture de votre projet

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

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

Activer le mode avancé AWS fonctionnalités

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Lorsque vous activez les fonctionnalités avancées, vous prenez le contrôle total de l' AWS organisation, du compte de gestion et du compte d'administrateur délégué utilisés pour gérer les projets que vous avez créés et les membres de l'équipe que vous avez invités. Vous gérerez directement la sécurité, la gouvernance et la composition de l'équipe de votre AWS environnement. Vous avez accès à des AWS services supplémentaires, à des fonctionnalités multirégionales et à des contrôles administratifs et de facturation améliorés.

Vous devez mettre à jour votre compte avant d'activer les fonctionnalités avancées. Pour plus d'informations, consultez Mettez à jour votre compte dans AWS Settings.

Que se passe-t-il lorsque vous activez les fonctionnalités avancées

Lorsque vous activez les fonctionnalités avancées, les modifications suivantes seront immédiatement appliquées à votre compte de gestion et à l' AWS organisation qui contient vos projets :

- Vous êtes désormais l'administrateur de l' AWS organisation qui contient vos projets.
- Vous avez défini une adresse e-mail root pour votre compte de gestion. Vous devrez également définir le mot de passe de l'utilisateur root. Pour plus d'informations, consultez Définissez un mot de passe utilisateur root pour votre compte de gestion.
- Vous gérez vos projets en tant que comptes membres au sein de votre organisation. En tant qu'administrateur de cette organisation, vous pouvez créer des comptes membres au sein de l'organisation. Votre AWS Builder ID reste propriétaire de vos comptes de projet. Pour plus d'informations, consultezComptes de projet après avoir activé les fonctionnalités avancées.
- Pour attribuer un rôle d'administrateur aux comptes des membres que vous invitez à rejoindre votre organisation, vous devez créer un OrganizationAccountAccessRole. Pour plus d'informations, voir Création du OrganizationAccountAccessRole dans un compte de membre invité.
- Les membres de votre équipe sont appelés « identités du personnel » et ils peuvent toujours accéder à vos AWS comptes. Vous pouvez également choisir de personnaliser la source d'identité de votre personnel à l'aide d'IAM Identity Center. Vous pouvez continuer à utiliser AWS Builder ID comme source d'identité, ou vous pouvez le remplacer par une source d'identité externe. Si vous modifiez votre source d'identité de AWS Builder ID à une autre source d'identité, c'est irréversible. Vous ne pourrez pas réactiver AWS Builder ID en tant que source d'identité à l'avenir. Pour plus d'informations, consultez Modifier la source d'identité à partir de AWS ID de créateur.
- Vous contrôlez AWS l'accès des utilisateurs et des groupes dans votre instance d'organisation IAM Identity Center à l'aide du gestionnaire d'accès aux comptes. Vous pouvez utiliser cette fonctionnalité pour modifier l'accès des utilisateurs, tout en leur permettant de se connecter `aws login` pour recevoir leurs informations d'identification de session de rôle IAM depuis le navigateur. Pour plus d'informations, consultez AWS Account Access Manager.
- AWS crée un compte membre appelé Identity Delegated Admin dans votre organisation avec un rôle d'administrateur délégué. Ce rôle est utilisé pour effectuer la plupart des tâches administratives dans le centre d'identité IAM et le gestionnaire d'accès aux comptes. Le rôle d'administrateur délégué doit être utilisé dans l'est des États-Unis (Virginie du Nord). Pour plus d'informations, consultez Administration déléguée.

  Votre AWS Builder ID possède le compte Identity Delegated Admin, comme les comptes de votre projet.
- Vous pouvez désormais configurer des politiques de contrôle des ressources (RCP) et des politiques de contrôle des services (SCP) pour appliquer des garde-fous personnalisés dans votre organisation. Auparavant, je AWS gérais les RCP et les SCP en votre nom. Vous pouvez modifier

ces politiques après avoir activé les fonctionnalités avancées. Pour plus d'informations, consultez Supprimer les politiques de l'organisation.

Lorsque vous activez les fonctionnalités avancées, les modifications suivantes sont également appliquées à votre AWS organisation :

- Si vous avez une limite de dépenses pour l'un de vos AWS comptes, elle est supprimée. Tous les projets actuellement en pause seront réactivés. Vous ne pouvez pas créer de limite de dépenses si vous activez les fonctionnalités avancées. Au lieu de cela, vous avez accès à l'ensemble de la suite d'outils de Billing and Cost Management. Cela inclut la définition des budgets, le téléchargement des rapports de l'explorateur de coûts et la détection des dépenses inhabituelles grâce à la détection des anomalies de AWS coûts. Vous pouvez utiliser ces outils avancés pour analyser, organiser, planifier et optimiser vos coûts.
- Vous pouvez accéder à tous les AWS services. Les services disponibles sont répertoriés dansthe section called "Services AWS non pris en charge pour notre nouveau AWS expérience". Vous devez planifier votre architecture et consulter la documentation du service avant d'activer ces services. En outre, Agent Toolkit fournit de nombreuses compétences pour travailler avec ces services.
- Vous avez accès à des régions supplémentaires Régions AWS, facultatives, ainsi qu'à des fonctionnalités multirégionales. Multi-Region l'architecture améliore la résilience de vos charges de travail. Nous vous recommandons de planifier la manière dont vous allez limiter et auditer votre empreinte régionale. Il est important de s'assurer que les ressources que vous créez ne sont présentes que dans les régions que vous avez l'intention d'utiliser.
- Vous pouvez désactiver le gestionnaire de rôles IAM pour chacun des membres Compte AWS de votre organisation. Le gestionnaire de rôles IAM est un paramètre de compte facultatif qui attribue automatiquement les rôles, de sorte que vous et votre personnel n'avez pas besoin de les configurer. Pour plus d'informations, consultez Comment activer et désactiver le gestionnaire de rôles (console).
- Vous pouvez utiliser IAM Access Analyzer.

Lorsque vous activez les fonctionnalités avancées, les modifications suivantes sont également appliquées à votre expérience utilisateur :

- Auparavant, il Console de gestion AWS affichait une vue simplifiée avec un menu que vous utilisiez pour passer d'un projet à l'autre et accéder aux AWS paramètres. Ils Console de gestion AWS s'étendent pour inclure des fonctionnalités supplémentaires telles que le sélecteur de

région, des services supplémentaires et la définition d'une couleur pour le compte à laquelle vous pouvez accéder pour les distinguer visiblement. Pour plus d'informations, consultez la section Fonctionnalités de la console.

- Vous pouvez désormais également effectuer les opérations suivantes :
  - Désactivez la prise en charge des consoles multisessions.
  - Désignez votre AWS compte comme étant conforme à la loi HIPAA ou à la SEC.
  - Utilisez AWS Marketplace.
  - Gagnez des crédits supplémentaires avec AWS Activate.
  - Travaillez avec un partenaire AWS de formation.
  - Achetez un abonnement à AWS Skill Builder Team.
  - Souscrivez un accord d'entreprise avec AWS.
  - Créez un contrat de services professionnels.
  - Rejoignez le réseau de AWS partenaires.

Comptes de projet après avoir activé les fonctionnalités avancées

Chaque projet que vous avez créé dans AWS les paramètres contient un Compte AWS compte appelé compte de projet. Un AWS Builder ID est propriétaire de chaque compte de projet au lieu de l'adresse e-mail de l'utilisateur root. Lorsque vous activez les fonctionnalités avancées, vos comptes de projet deviennent des comptes de membres de votre organisation, et votre AWS Builder ID continue de les détenir, même si vous modifiez ultérieurement votre source d'identité. Votre AWS Builder ID possède également le compte Identity Delegated Admin qui est AWS créé lorsque vous activez des fonctionnalités avancées.

Étant donné qu'un compte de projet ne possède pas d'adresse e-mail d'utilisateur root, il fonctionne différemment des autres comptes membres de votre organisation :

- L'adresse e-mail affichée sur la AWS Organizations console pour un compte de projet est un espace réservé qui est AWS généré. Les `GetPrimaryEmail` opérations `DescribeAccount`,`ListAccounts`,`ListAccountsForParent`,`ListDelegatedAdministrators`, et renvoient le même espace réservé. Il ne s'agit pas d'une adresse e-mail que vous pouvez utiliser ou modifier.
- Vous ne pouvez pas mettre à jour l'adresse e-mail de l'utilisateur root d'un compte de projet. Les appels vers `StartPrimaryEmailUpdate` ou `AcceptPrimaryEmailUpdate` pour un compte

de projet échouent avec une `AccessDeniedException` erreur, même lorsque l'appelant dispose des autorisations requises.

- Vous ne pouvez pas vous connecter à un compte de projet en tant qu'utilisateur root ni récupérer son mot de passe utilisateur root.
- Vous ne pouvez pas supprimer un compte de projet de votre organisation, et il ne peut pas quitter votre organisation ou rejoindre une autre organisation. Si vous `RemoveAccountFromOrganization` demandez un compte de projet, l'appel échoue avec un `ConstraintViolationException` message d'erreur indiquant que le compte appartient à un Builder ID.

Pour arrêter d'utiliser un compte de projet, fermez-le de votre compte de gestion. Comme vous ne pouvez pas supprimer de comptes de projet de votre organisation, vous ne pouvez supprimer votre organisation qu'une fois que tous vos comptes de projet, y compris le compte Identity Delegated Admin, ont été définitivement fermés. AWS ferme définitivement un compte lorsque la période de 90 jours suivant sa fermeture prend fin.

Les comptes membres que vous créez dans votre organisation après avoir activé les fonctionnalités avancées ont une adresse e-mail d'utilisateur root, et ces différences ne s'appliquent pas à eux. Si vous avez besoin d'un compte dont vous pouvez modifier l'adresse e-mail de l'utilisateur root ou que vous pouvez supprimer ultérieurement de votre organisation, créez un nouveau compte membre et transférez vos ressources vers celui-ci.

Comment va AWS Les paramètres changent-ils après avoir activé les fonctionnalités avancées ?

Après avoir activé les fonctionnalités avancées, AWS les paramètres seront disponibles tant que vous utiliserez AWS Builder ID comme source d'identité. AWS Les paramètres ne seront accessibles qu'à partir de https://settings.aws.com. Vous ne pourrez pas y accéder depuis le Console de gestion AWS. AWS Les paramètres fourniront des liens permettant de gérer votre compte à l'aide de votre compte de gestion. Avec votre compte de gestion, vous pouvez accéder aux Console de gestion AWS emplacements suivants dans les AWS paramètres. Utilisez le compte de gestion uniquement pour effectuer des tâches administratives, notamment :

- Accédez à la console Billing and Cost Management pour consulter vos informations de facturation.
- Accédez à la console d' AWS organisation pour modifier les SCP et RCP qui régissent votre organisation.

- Accédez à la console AWS Account Access Manager pour modifier l'accès détaillé à l'identité de vos employés.
- Accédez au centre d'identité IAM pour modifier votre source d'identité.

Utilisez le compte de gestion pour effectuer ces tâches. Bien que vous ayez également accès à l'adresse e-mail et au mot de passe de l'utilisateur root, nous vous recommandons de n'utiliser vos informations d'identification d'utilisateur root que pour un accès d'urgence à votre compte.

Vous pouvez également utiliser AWS les paramètres pour accéder à vos AWS comptes au sein de votre organisation et à tout projet partagé avec vous.

Si vous souhaitez créer des rôles personnalisés et y accéder depuis les AWS paramètres de vos comptes, vous devez définir une durée de session de 12 heures.

Si les membres de votre équipe ont accès à un projet, vous pouvez le consulter et y accéder de la même manière qu'avant d'activer les fonctionnalités avancées. Les projets partagés avec vous ne sont pas affectés si vous activez les fonctionnalités avancées pour votre propre compte de gestion et votre AWS organisation.

Puis-je tout de même créer un projet dans AWS Réglages après avoir activé les fonctionnalités avancées ?

Vous ne pouvez pas créer de projet dans votre AWS organisation actuelle après avoir activé les fonctionnalités avancées. Vous devez créer un compte membre dans votre organisation.

Vous pouvez créer une nouvelle AWS organisation gérée avec des paramètres par défaut préconfigurés. Pour ce faire, créez un nouveau projet dans AWS Réglages. Vous pouvez ensuite créer des projets supplémentaires et inviter les membres de l'équipe à collaborer. Vous pouvez également activer les fonctionnalités avancées pour ce compte de gestion.

Le nouvel environnement préconfiguré auquel vous accédez n'aura aucun lien avec AWS l'organisation précédente créée lors de votre première inscription AWS.

Comment se préparer à activer les fonctionnalités avancées

Nous vous recommandons de procéder comme suit avant d'activer les fonctionnalités avancées :

- Informez tous les membres de votre équipe que vous allez activer des fonctionnalités avancées. À moins que vous ne modifiiez les paramètres, les membres de votre équipe auront le même

accès aux projets, mais la Console de gestion AWS vue simplifiée sera remplacée par une vue qui montre les régions et donne accès à davantage de services. Si vous modifiez ultérieurement la source d'identité ou si vous ajoutez de nouveaux SCP ou RCP, informez-en votre personnel, car ces modifications peuvent affecter la manière dont ils se connectent et les accès auxquels ils peuvent accéder.

- Consultez les dépenses de tous vos projets en cours et notez si certains projets contiennent des coûts qui fluctuent de manière significative. Sans limite de dépenses, vous serez responsable de tous les coûts engagés par vos ressources. Nous vous recommandons de supprimer ou de suspendre les ressources inactives avant d'activer les fonctionnalités avancées.
- Planifiez les changements que vous allez apporter à vos AWS organisations et recherchez les meilleures pratiques. Si vous envisagez de créer des ressources dans un autre pays Région AWS, modifiez la politique de contrôle des services appliquée à tous les utilisateurs afin de les restreindre Régions AWS. Vous devez modifier le StatementID `RegionFloor` pour inclure de nouvelles régions. Pour plus d'informations, consultez Politiques de contrôle des services pour les projets.
- Si vous avez suivi les étapes décritesConnectez un outil de codage basé sur l'IA, votre outil d'IA dispose d'un contexte uniquement relatif à la nouvelle AWS expérience. Cela peut entraîner des problèmes au fur et à mesure que vous développez à l'aide de fonctionnalités avancées. Nous vous recommandons la procédure suivante :
  - Supprimez le `aws-starter-rules.md` fichier de l'emplacement où vous l'avez enregistré. Le fichier de règles a été enregistré en fonction de votre agent. Pour plus d'informations, voir Où placer le fichier de règles.

Comment activer les fonctionnalités avancées

Vous pouvez activer les fonctionnalités avancées dans AWS les paramètres. L'activation ne peut pas être annulée.

Pour activer les fonctionnalités avancées

1. Ouvrez AWS les paramètres sur https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Projects.
3. Pour Actions, choisissez Découvrir les fonctionnalités avancées.

   Comme l'activation ne peut pas être annulée, nous vous donnerons plus de temps pour explorer et en apprendre davantage sur le processus d'activation.
4. Lorsque vous êtes prêt à l'activer, procédez comme suit :

a. Dans Nom de l'équipe, entrez le nom de l'équipe. Il s'agit du nom de l'instance IAM Identity Center utilisée pour stocker les identités de vos employés. Vos employés verront ce nom.
b. Pour Choisir l'adresse e-mail du compte de gestion, choisissez une adresse e-mail. Cette adresse e-mail est utilisée pour accéder au compte de gestion et effectuer des tâches. Si vous utilisez une adresse e-mail différente, l'e-mail AWS Builder ID aura toujours accès au compte de gestion depuis AWS les paramètres, à condition que vous utilisiez toujours AWS Builder ID comme source d'identité.
c. Terminez le processus de vérification de l'adresse e-mail du compte de gestion.
d. Choisissez Réviser et terminez l'activation.
e. Confirmez votre choix, puis sélectionnez Activer. Dans ce cas, vous ne pourrez pas rétablir votre compte.

Félicitations, vous avez activé les AWS fonctionnalités avancées !

Après avoir activé les fonctionnalités avancées

Après avoir activé les fonctionnalités avancées, vous pouvez effectuer les opérations suivantes :

- Gérer les membres du personnel
- Modifier la source d'identité à partir de AWS ID de créateur
- Supprimer les politiques de l'organisation
- Création d'une unité organisationnelle
- Activez ou désactivez Régions AWS dans votre compte
- Création de rôles IAM

Définissez un mot de passe utilisateur root pour votre compte de gestion

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Après avoir activé les fonctionnalités avancées, votre compte de gestion utilise désormais une adresse e-mail root pour le récupérer. Bien que vous puissiez toujours récupérer l'accès à votre

AWS Builder ID à l'aide des options en libre-service pour récupérer l'accès, vous pouvez désormais récupérer l'accès à votre compte de gestion avec les informations d'identification de l'utilisateur root. Pour accéder à l'utilisateur root, vous devez créer un mot de passe utilisateur root. En outre, nous vous recommandons d'activer l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre utilisateur root.

Pour définir un mot de passe utilisateur root

1. Ouvrez la console AWS de gestion et choisissez Se connecter à l'aide de l'adresse e-mail de l'utilisateur root.
2. Dans Adresse e-mail, entrez l'adresse e-mail de l'utilisateur root.

   Il s'agit de l'adresse e-mail que vous avez définie pour le compte de gestion lorsque vous avez activé les fonctionnalités avancées.
3. Choisissez Forgot your password? (Mot de passe oublié ?).

   Le processus de réinitialisation du mot de passe permet également de définir le mot de passe de votre utilisateur root après avoir activé les fonctionnalités avancées.
4. Entrez l'adresse e-mail associée au compte.
5. Entrez le texte du CAPTCHA et choisissez Je ne suis pas un robot.
6. Vérifiez que l'e-mail qui vous est associé ne contient Compte AWS pas de message provenant d'Amazon Web Services. L'e-mail peut provenir d'une adresse se terminant par dans `@verify.signin.aws`. Suivez les instructions contenues dans l'e-mail pour définir un mot de passe utilisateur root. Si vous ne voyez pas l'e-mail dans votre compte, vérifiez le dossier des courriers indésirables. Si vous n'avez plus accès à l'e-mail, consultez la section Je n'ai pas accès à l'e-mail associé à mon AWS compte dans le guide de AWS Sign-In l'utilisateur.

Une fois que vous avez défini le mot de passe de l'utilisateur root, vous pouvez récupérer l'accès à votre compte. Suivez ensuite les instructions relatives à l'Multi-factor authentification pour l'utilisateur root du AWS compte afin d'activer le MFA pour vos informations d'identification root.

N'utilisez l'utilisateur root que pour récupérer votre compte ou lorsque cela est nécessaire pour effectuer des tâches nécessitant des informations d'identification de l'utilisateur root. Pour le travail quotidien, connectez-vous avec votre source d'identité, telle que AWS Builder ID.

Gérer les membres du personnel

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Après avoir activé les fonctionnalités avancées, vous pouvez inviter de nouveaux membres du personnel ou supprimer des membres existants. Cela inclut l'ajout de votre personnel existant à de nouveaux AWS comptes. Les informations suivantes concernent uniquement les AWS organisations qui utilisent AWS Builder ID comme source d'identité. Si vous faites appel à un fournisseur d'identité externe (IdP), vous gérez votre personnel au sein de ces fournisseurs d'identité. Si vous utilisez le répertoire Identity Center, consultez la documentation décrite dans Gérer les utilisateurs dans le répertoire Identity Center.

Pour inviter de nouveaux membres du personnel

1. Ouvrez AWS les paramètres sur https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Projects.
3. Accédez à la AWS console de votre compte d'administrateur délégué aux identités.
4. Depuis AWS la page d'accueil de la console, recherchez-la **`IAM Identity Center`** et choisissez-la.
5. Sur la page Utilisateurs de la console IAM Identity Center, choisissez Inviter un nouveau membre de l'équipe.
6. Pour E-mail, entrez une adresse e-mail ou une liste d'adresses e-mail. Séparez les adresses e-mail par des virgules (,) ou des points-virgules (;).
7. Choisissez Send invitation (Envoyer une invitation).

Pour accorder à un nouveau membre du personnel l'accès à AWS comptes

Une fois que le membre du personnel a accepté son invitation, vous configurez AWS les comptes auxquels il a accès.

Accordez des autorisations complètes à un compte que vous avez créé avant d'activer les fonctionnalités avancées

1. Identifiez l'identifiant du compte auquel vous souhaitez accorder l'accès. Pour trouver l'identifiant du compte, voir Afficher les identifiants de AWS compte.
2. Dans le volet de navigation principal, choisissez Groups.
3. Sélectionnez le nom du groupe qui commence par l'identifiant de compte que vous avez identifié.
4. Choisissez Ajouter des utilisateurs au groupe.
5. Sélectionnez l'utilisateur que vous souhaitez ajouter.
6. Choisissez Ajouter un utilisateur.

Accorder des autorisations personnalisées à une personne nouvelle ou existante AWS compte

Vous configurez l'accès personnalisé dans le Gestionnaire d'accès au AWS compte. Pour plus d'informations, voir Gérer l'accès aux AWS comptes.

> **Note**
>
> Si vous souhaitez créer des rôles personnalisés et leur accorder l'accès à partir des AWS paramètres, vous devez définir la durée de la session à 12 heures.

Pour supprimer des membres du personnel

1. Ouvrez AWS les paramètres sur https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Projects.
3. Pour Actions, sélectionnez Gérer l'équipe.

   Cela ouvrira le centre d'identité IAM.
4. Sur la page Utilisateurs de la console IAM Identity Center, sélectionnez un membre de l'équipe, puis choisissez Supprimer.
5. Confirmez votre choix et choisissez Supprimer.

Le membre de l'équipe perdra immédiatement tout accès à votre AWS organisation.

Ces étapes vous montrent comment gérer les membres de votre personnel en accédant d'abord aux AWS paramètres. Cependant, vous pouvez vous connecter à l' Console de gestion AWS aide de votre compte d'administrateur délégué et accéder à l'IAM Identity Center ou à la console IAM pour gérer les membres de votre personnel.

Modifier la source d'identité à partir de AWS ID de créateur

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Après avoir activé les fonctionnalités avancées, vous pouvez modifier votre source d'identité depuis AWS Builder ID. Si vous modifiez votre source d'identité à partir de AWS Builder ID, vous ne pourrez jamais réutiliser AWS Builder ID comme source d'identité pour votre AWS organisation. La modification de votre source d'identité modifie la façon dont vos employés se connectent. Votre AWS Builder ID reste propriétaire de vos comptes de projet.

Pour modifier votre source d'identité à partir de AWS ID de créateur

1. Ouvrez AWS les paramètres sur https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Projects.
3. Dans Gérer cette organisation, choisissez Modifier la source d'identité.

   Cela ouvrira le centre d'identité IAM.
4. Sur la page Paramètres de la console IAM Identity Center, choisissez Actions, puis Modifier la source d'identité.
5. Pour Choisir une source d'identité, le AWS Builder ID sera sélectionné. Choisissez une nouvelle source, puis cliquez sur Suivant.
6. Si vous passez à Active Directory, choisissez le répertoire disponible dans le menu de la page suivante. Si vous passez à un fournisseur d'identité externe, nous vous recommandons de suivre les étapes décrites dans Comment se connecter à un fournisseur d'identité externe.
7. Vérifiez et confirmez vos modifications. Vous devrez cocher toutes les cases pour confirmer que vous comprenez les modifications apportées à votre organisation.
8. Confirmez votre choix et choisissez Modifier la source d'identité.

Ces étapes vous montrent comment modifier votre source d'identité en accédant d'abord aux AWS paramètres. Cependant, vous pouvez vous connecter à l' Console de gestion AWS aide de votre compte d'administrateur délégué et accéder au centre d'identité IAM pour modifier votre source d'identité.

Supprimer les politiques de l'organisation

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Après avoir activé les fonctionnalités avancées, vous pouvez modifier les politiques de contrôle des ressources (RCP) et les politiques de contrôle des services (SCP) pour modifier la gouvernance de votre AWS organisation. Certaines politiques organisationnelles AWS gérées sont supprimées lorsque vous activez des fonctionnalités avancées. Pour de plus amples informations, veuillez consulter Politiques gérées pour votre organisation. Les informations suivantes concernent uniquement les AWS organisations qui utilisent AWS Builder ID comme source d'identité. Si vous utilisez une autre source, suivez les étapes décrites dans la section Mettre à jour une politique.

Pour modifier une politique de contrôle des services (SCP)

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Projets.
3. Dans Gérer cette organisation, choisissez Gérer les politiques.

   Cela va ouvrir la AWS Organizations console.
4. Choisissez la page Politique de contrôle des services.
5. Choisissez le nom de la politique que vous souhaitez mettre à jour.
6. Sur la page des détails de la politique, choisissez Modifier la politique.
7. Effectuez une ou plusieurs des modifications suivantes :

   - Vous pouvez renommer la politique en saisissant un nouveau nom dans Nom de la politique.
   - Vous pouvez en changer la description en saisissant un nouveau texte dans Description de la politique.

- Vous pouvez modifier le texte de la politique en modifiant la politique au format JSON dans le panneau de gauche. Par ailleurs, vous pouvez choisir une instruction dans l'éditeur situé à droite et en modifier les éléments à l'aide des commandes. Pour de plus amples informations sur chaque contrôle, consultez Création d'une procédure SCP plus haut dans cette rubrique.

8. Lorsque vous avez terminé, choisissez Enregistrer les modifications.

Pour modifier une politique de contrôle des ressources (RCP)

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Projets.
3. Dans Gérer cette organisation, choisissez Gérer les politiques.

   Cela va ouvrir la AWS Organizations console.
4. Choisissez la page Politique de contrôle des ressources.
5. Choisissez le nom de la politique que vous souhaitez mettre à jour.
6. Sur la page des détails de la politique, choisissez Modifier la politique.
7. Effectuez une ou plusieurs des modifications suivantes :

   - Vous pouvez renommer la politique en saisissant un nouveau nom dans Nom de la politique.
   - Vous pouvez en changer la description en saisissant un nouveau texte dans Description de la politique.
   - Vous pouvez modifier le texte de la politique en modifiant la politique au format JSON dans le panneau de gauche. Par ailleurs, vous pouvez choisir une instruction dans l'éditeur situé à droite et en modifier les éléments à l'aide des commandes. Pour plus de détails sur chaque contrôle, consultez la procédure Création d'un RCP plus haut dans cette rubrique.

8. Lorsque vous avez terminé, sélectionnez Enregistrer les modifications.

Ces étapes vous montrent comment modifier les politiques de l'organisation par AWS paramètres. Cependant, vous pouvez vous connecter à l' Console de gestion AWS aide de votre compte de gestion et accéder à la AWS Organizations console pour modifier ces politiques.

Fermez votre compte dans AWS Settings

> **Warning**
>
> Nous proposons actuellement notre nouvelle expérience à un nombre limité de clients. Il se peut que vous ne puissiez pas encore accéder à cette expérience.

Si vous n'avez plus besoin de l'organisation et de tous les projets qui y sont stockés, vous pouvez fermer vos projets, fermer votre compte de gestion et supprimer votre AWS Builder ID.

Pour vous assurer que les AWS ressources que vous consommez ne vous sont plus facturées, vous devez fermer vos projets et fermer le compte de gestion de votre organisation, mais vous n'êtes pas obligé de fermer votre AWS profil. Le AWS Builder ID qui y est associé est gratuit.

Après avoir fermé votre compte de gestion, vous pouvez le rouvrir dans les 90 jours à compter du jour où vous l'avez fermé. La période qui s'écoule entre le jour où vous avez fermé le compte de gestion et la date de fermeture AWS définitive du compte de gestion correspond à la période qui suit la clôture.

Ce que vous devez savoir avant de fermer votre compte de gestion

Avant de fermer votre compte de gestion, vous devez prendre en compte les points suivants :

- Lorsque vous clôturez un projet, tenez compte des considérations figurant dansCe que vous devez savoir avant de clôturer votre projet.
- Vous devez fermer tous les projets avant de pouvoir fermer votre compte de gestion.
- Vous devez fermer votre compte de gestion avant de supprimer votre AWS Builder ID.
- Après avoir fermé votre compte de gestion, vous pouvez le rouvrir dans les 90 jours à compter du jour où vous l'avez fermé. La période qui s'écoule entre le jour où vous avez fermé le compte de gestion et la date de fermeture AWS définitive du compte de gestion correspond à la période qui suit la clôture.
- Vous pouvez rouvrir votre compte après la fermeture.
- Vous ne pouvez pas utiliser la même adresse e-mail que celle enregistrée auprès de votre organisation au moment de sa fermeture comme adresse e-mail principale d'une autre organisation. Si vous souhaitez utiliser la même adresse e-mail pour une autre organisation lorsque vous utilisez S'inscrire pour AWS (nouveau), nous vous recommandons de la mettre à jour avant la

fermeture. Pour de plus amples informations, veuillez consulter Changez votre adresse e-mail dans AWS Settings.

- Si vous avez activé l'authentification multifacteur (MFA) sur votre compte de gestion et configuré un appareil MFA, l'AMF n'est pas automatiquement supprimée lorsque vous fermez le compte de gestion. Si vous choisissez de laisser l'authentification multifacteur activée pendant les 90 jours suivant la fermeture, laissez l'appareil MFA actif jusqu'à l'expiration de cette période, au cas où vous auriez besoin d'accéder au compte pendant cette période. Notez que les appareils 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 matériel TOTP avec un autre utilisateur ultérieurement, vous avez la possibilité de désactiver le périphérique MFA matériel avant de fermer le compte de gestion.

Fermer un projet

Pour clôturer vos projets, consultezFermer un projet dans AWS Settings.

Fermez votre compte de gestion

Pour fermer votre compte de gestion

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.
2. Dans le volet de navigation principal, choisissez Project.
3. Pour Actions, choisissez Fermer le compte de gestion.
4. Confirmez votre choix et choisissez Fermer le compte de gestion.

Supprimez votre AWS ID de créateur

La suppression de votre AWS Builder ID aura les conséquences suivantes :

- Perte d'accès : outre votre projet et votre organisation, vous ne pouvez plus accéder aux AWS outils et services auxquels vous avez accédé auparavant via AWS Builder ID.
- Suppression de contenu : tout contenu restant associé uniquement à votre AWS Builder ID sera supprimé et vous ne pourrez plus accéder à votre contenu ni le récupérer depuis les applications utilisant votre AWS Builder ID.
- Suppression des informations personnelles : toutes les informations personnelles que vous avez fournies dans le cadre de la création et de la gestion de votre identifiant de AWS constructeur

seront supprimées, sauf celles qui AWS peuvent conserver des informations personnelles conformément à la loi, telles que les enregistrements de votre demande de suppression ou les données sous une forme qui ne permet pas de vous identifier.

Vous pouvez en savoir plus sur la manière dont nous traitons vos informations dans la AWS Politique de confidentialité. Vous pouvez mettre à jour vos préférences AWS de communication ou vous désabonner en vous rendant dans le Centre AWS des préférences de communication.

Les identifiants existants restent inchangés : si vous utilisez un identifiant tel que Google ou Apple, la suppression de votre AWS Builder ID ne supprime rien de votre compte de connexion.

Pour supprimer votre AWS ID de créateur

1. Ouvrez AWS les paramètres à l'adresse https://settings.aws.com.

   Même si vous avez supprimé votre compte de gestion, vous pouvez toujours vous connecter.
2. Dans le volet de navigation principal, choisissez Gérer le profil.
3. Pour les informations de profil, choisissez Gérer le profil.

   Vous serez redirigé vers votre profil AWS Builder ID.
4. Dans le volet de navigation principal, choisissez Confidentialité et données.
5. Pour supprimer AWS Builder ID, choisissez Supprimer votre AWS Builder ID.
6. Confirmez votre choix et choisissez Supprimer.

Inscrivez-vous pour AWS (avancé)

Si vous êtes nouveau AWS, la première étape consiste à vous inscrire à un Compte AWS. Lorsque vous suivez les instructions de Sign up for AWS (advanced), vous AWS créez un compte dans lequel vous avez un contrôle total sur la configuration du compte et sur l'emplacement de stockage de votre contenu. Utilisez cette option si vous avez des charges de travail réglementées telles que HIPAA ou FedRAMP.

Pour comparer cet abonnement avec Sign up for AWS (nouveau), voirComparez les options d'inscription.

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.
- 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 leur attribuer des noms faciles à reconnaître. Pour les comptes d'entreprise, pensez à utiliser une norme de dénomination telle que organisation - objectif - environnement (par exemple, AnyCompany- audit - production). Pour les comptes personnels, pensez à utiliser une norme de dénomination telle que prénom, nom de famille, fonction (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 est utilisé à des fins de vérification d'identité et pour confirmer la propriété de votre compte. Vous devez être en mesure de recevoir des appels et des SMS à ce numéro de téléphone.

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

Étape 1 : Créez votre compte

Ces instructions concernent la création d'une zone Compte AWS en dehors de l'Inde. Pour créer un compte en Inde, Créez un Compte AWS avec AWS Inde voir. Pour créer un compte faisant partie d'une organisation gérée par AWS Organizations, voir Création d'un compte membre dans une organisation dans le Guide de l'AWS Organizations utilisateur.

Console de gestion AWS

Pour créer un Compte AWS

1. Ouvrez la AWS page d'inscription.
2. Entrez l'adresse e-mail et le Compte AWS nom de l'utilisateur root, puis choisissez Vérifier l'adresse e-mail. Cela envoie un code de vérification à votre adresse e-mail.

   > **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.

3. Entrez votre code de vérification, puis choisissez Vérifier.
4. 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.

5. Choisissez le plan de votre compte. Pour plus d'informations, consultez la section Forfaits de niveau gratuit.
6. Entrez vos coordonnées, puis lisez et acceptez le contrat AWS client. Assurez-vous de bien comprendre les conditions avant d'accepter.

> **Important**
>
> Si ce compte est destiné à une entreprise, il est recommandé de saisir le numéro de téléphone de l'entreprise plutôt que le numéro d'un téléphone personnel. 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.

7. Entrez vos informations de facturation. 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.
8. Il se peut que vous deviez confirmer votre identité :

   a. Pour le code du pays ou de la région, entrez un numéro de téléphone joignable dans les prochaines minutes.

   b. Dans Numéro de téléphone, entrez un numéro de téléphone joignable dans les prochaines minutes.

   c. Choisissez Envoyer un SMS.

   d. Lorsque le système automatique vous contacte, entrez le code que vous recevez, puis choisissez Continuer.
9. Choisissez 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.
10. Choisissez Terminer l'inscription. Une page de confirmation s'affiche pour indiquer que votre compte est en cours d'activation.

11. 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.
12. Après avoir reçu le message d'activation, vous pouvez vous connecter au pour commencer Console de gestion AWSà l'utiliser Services AWS. Pour obtenir des informations générales sur la façon de gérer les paramètres de votre compte, consultezConfigurez votre Compte AWS.

En cas de Comptes AWS gestion multiple AWS Organizations, attribuez un accès administratif à un utilisateur administratif dans IAM Identity Center. 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.

AWS CLI & SDKs

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

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

Étape 2 : (recommandé) Installez le AWS CLI

Installez le AWS CLI en suivant les instructions de la section Installation du AWS CLI. Vous avez besoin de la version 2.32.0 ou ultérieure.

Vous pouvez utiliser le AWS CLI pour qu'un agent gère les AWS ressources en votre nom.

Après avoir installé le AWS CLI, utilisez la commande suivante pour vous connecter par programmation :

```
aws login
```

Cela change automatiquement vos informations d'identification toutes les 15 minutes, ce qui permet à votre session de rester valide jusqu'à 12 heures sans intervention manuelle.

Utilisez la commande suivante pour vérifier que vos informations d'identification fonctionnent :

```
aws sts get-caller-identity
```

Pour plus d'informations sur l'accès à votre Compte AWS, consultezAccès à votre Compte AWS.

Étape 3 : (Recommandé) Configurez le AWS Serveur MCP

Le serveur AWS MCP est un serveur géré auquel les agents peuvent accéder AWS via le protocole MCP (Model Context Protocol). Les agents peuvent effectuer des recherches dans AWS la documentation et récupérer des informations de service sans authentification. Pour exécuter des appels d' AWS API, exécuter des scripts Python dans un environnement sandbox ou suivre des compétences sélectionnées, les agents s'authentifient via vos informations d'identification IAM existantes. Pour plus d'informations, voir Qu'est-ce que le kit d'outils pour AWS agents ?

Une fois le processus d'inscription terminé, consultez les rubriques suivantes :

- Connexe AWS services
- Utilisation de Utilisateur racine d'un compte AWS
- Accès à votre Compte AWS
- Planifiez votre Compte AWS structure de gouvernance
- Configurez votre Compte AWS
- Résolvez vos problèmes Compte AWS
- Gérer des comptes en Inde
- Fermez un Compte AWS
- Réouvrir un Compte AWS

Connexe AWS services

Selon la manière dont vous vous inscrivez AWS, vous avez accès à des projets Comptes AWS ou à des projets. Les projets contiennent Comptes AWS et les paramètres de partage avec d'autres collaborateurs. Pour de plus amples informations, veuillez consulter Comparez les options d'inscription. Dans cette section, nous expliquons comment Comptes AWS vous pouvez créer à l'aide de Sign up for AWS (advanced) pour fonctionner de manière fluide avec les services suivants :

- IAM

Compte AWS Le vôtre est étroitement intégré à Gestion des identités et des accès AWS (IAM). Vous pouvez utiliser IAM avec votre compte pour vous assurer que les autres personnes qui travaillent sur votre compte disposent de l'accès dont elles ont besoin pour effectuer leur travail. Vous utilisez également IAM pour contrôler l'accès à toutes vos AWS ressources, et pas seulement aux informations spécifiques à votre 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 mise en place 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 se développer, vous souhaiterez peut-être créer 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 multicomptes. 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 l'utiliser AWS Organizations.

  Les actions d'API suivantes liées au compte font partie de l' AWS Organizations API, et non de l'API de gestion de AWS compte. Nous les incluons ici car les clients recherchent généralement ces opérations dans la documentation de gestion des comptes, mais elles sont définies dans l' AWS Organizations espace de noms.

  - CreateAccount
  - CreateGovCloudAccount
  - DescribeAccount

- 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 à l'aide AWS Organizations de l'instanciation d'un ensemble de comptes initiaux et de certaines barrières et configurations par défaut pour l'environnement. Vous pouvez l'utiliser AWS Control Tower pour approvisionner de nouveaux comptes 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 l'utiliser AWS Control Tower.

Utilisation de Utilisateur racine d'un compte AWS

Selon la manière dont vous vous inscrivez AWS, vous avez accès à des projets Comptes AWS ou à des projets. Les projets contiennent Comptes AWS les paramètres de partage avec d'autres collaborateurs. Pour plus d'informations, consultez Comparez les options d'inscription. Dans cette section, nous expliquons comment utiliser l'utilisateur root dans un fichier Compte AWS que vous créez à l'aide de Sign up for AWS (avancé). Un AWS Builder ID est propriétaire de chaque compte de projet au lieu d'une adresse e-mail d'utilisateur root. Vous ne pouvez donc pas utiliser l'utilisateur root dans un compte de projet, y compris après avoir activé les fonctionnalités avancées.

Lorsque vous créez un Compte AWS, vous commencez par une seule identité de connexion appelée utilisateur Compte AWS root qui dispose d'un accès complet à toutes Services AWS les ressources. Il est vivement déconseillé d'utiliser l'utilisateur racine pour vos tâches quotidiennes. Pour les tâches qui requièrent des informations d'identification de l'utilisateur racine, consultez Tâches qui requièrent les informations d'identification de l'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 (identifiants de clé d'accès et clés d'accès secrètes) pour votre utilisateur root. Pour obtenir de l'aide pour vous connecter en utilisant votre utilisateur root, voir Se connecter en Console de gestion AWS tant qu'utilisateur root dans le guide de AWS Sign-In l'utilisateur.

Accès à votre Compte AWS

Ces informations concernent l'accès à votre compte Compte AWS si vous vous êtes inscrit à AWS l'aide de Sign up for AWS (avancé) ou si vous avez activé des fonctionnalités avancées pour votre compte. Pour comparer les options d'inscription, consultezComparez les options d'inscription.

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

Console de gestion AWS

Console de gestion AWSIl 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

Les outils de ligne de AWS commande vous permettent d'émettre des commandes sur la ligne de commande de votre système pour effectuer 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 de 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 Outils AWS pour PowerShell l'utilisateur.

AWS Kits SDK

Les AWS SDK se composent de bibliothèques et d'exemples de code pour divers langages de programmation et plates-formes (par exemple, Java, Python, Ruby, .NET, iOS et Android). Ils automatisent les tâches telles que la signature cryptographique des demandes, la gestion des erreurs et les nouvelles tentatives de demande automatiques. Pour plus d'informations sur les AWS kits SDK, 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 des AWS comptes 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 Compte AWS structure de gouvernance

Ces informations concernent la planification de votre structure de Compte AWS gouvernance si vous vous êtes inscrit pour AWS utiliser Sign up for AWS (advanced) ou si vous avez activé

des fonctionnalités avancées pour votre compte. Pour comparer les options d'inscription, consultezComparez les options d'inscription.

Bien que vous ayez peut-être commencé votre AWS parcours avec un seul compte, nous vous AWS recommandons de configurer plusieurs comptes à mesure que la taille et la complexité de vos charges de travail augmentent. Que vous soyez une moyenne ou une grande entreprise, vous souhaiterez créer un plan de structure de gouvernance qui garantira la satisfaction de vos besoins en matière de données et de charge de travail.

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
- Quand l'utiliser AWS Organizations
- Quand l'utiliser AWS Control Tower
- Comprendre les modes de fonctionnement des API

Avantages de l'utilisation de plusieurs Comptes AWS

Ces informations concernent les avantages de l'utilisation multiple Comptes AWS si vous vous êtes inscrit pour AWS utiliser Sign up for AWS (avancé) ou si vous avez activé des fonctionnalités avancées pour votre compte. Pour comparer les options d'inscription, consultezComparez les options d'inscription.

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

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

- Contrôle de sécurité : 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 pouvoir en désigner un 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 contenus dans et Compte AWS sans affecter les autres. Les besoins de sécurité peuvent être différents en raison de différentes équipes ou de 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 cette banque de données et la gérer. Cela permet de limiter l'exposition à des données hautement confidentielles et peut donc contribuer à la conformité avec le 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 articles au niveau de la facturation. Les comptes multiples permettent de séparer les éléments au niveau de la facturation entre les unités commerciales, les équipes fonctionnelles ou les utilisateurs individuels. Vous pouvez toujours regrouper toutes vos factures auprès d'un seul payeur (en utilisant AWS Organizations la facturation consolidée) tout en séparant les rubriques par Compte AWS.
- Allocation de quotas : les quotas de AWS service sont appliqués séparément pour chacun Compte AWS. La séparation des charges de travail en différentes Comptes AWS catégories les empêche de consommer des quotas les uns pour les autres.

Toutes les recommandations et procédures décrites dans ce document sont conformes au AWS Well-Architected Cadre. 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 vous conformer à ces directives du framework. 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 Organizations, qui est un AWS service gratuit pour gérer l'ensemble des activités Comptes AWS de votre organisation.

AWS propose également AWS Control Tower, qui ajoute des couches d'automatisation AWS gérée aux organisations 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 l'utiliser AWS Organizations
- Quand l'utiliser AWS Control Tower

Quand l'utiliser AWS Organizations

Ces informations indiquent quand les utiliser AWS Organizations si vous vous êtes inscrit pour AWS utiliser Sign up for AWS (avancé) ou si vous avez activé des fonctionnalités avancées pour votre compte. Pour comparer les options d'inscription, consultezComparez les options d'inscription.

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 gérées par un seul payeur. Vous pouvez également gérer de manière centralisée la sécurité de votre organisation à l'aide de contrôles basés sur des politiques. Pour plus d'informations à ce sujet 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 peuvent être effectuées uniquement par le compte de gestion de l'organisation. Par défaut, cela inclut uniquement les opérations liées à la gestion de l'organisation elle-même. Vous pouvez étendre cette fonctionnalité supplémentaire à d'autres AWS services en activant un accès sécurisé entre les organisations et ce service. L'accès sécurisé autorise le AWS service spécifié à accéder aux informations relatives à l'organisation et aux comptes qu'elle contient. Lorsque vous activez l'accès sécurisé pour la gestion des comptes, le service de gestion

des comptes accorde aux organisations et à leur compte de gestion les autorisations nécessaires pour accéder aux métadonnées, telles que les informations de contact principales ou secondaires, pour tous les comptes membres de l'organisation.

Pour de plus amples informations, veuillez consulter Activez un accès sécurisé pour AWS Gestion du compte.

Administrateur délégué

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

Pour de plus amples informations, veuillez consulter Activer un compte administrateur délégué pour AWS Gestion du compte.

Politiques de contrôle des services

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

Par exemple, les SCP qui s'appliquent à Comptes AWS, voirRestreindre l'accès en utilisant AWS Organizations politiques de contrôle des services.

Activez un accès sécurisé pour AWS Gestion du compte

Ces instructions expliquent comment activer l'accès sécurisé pour la gestion de AWS compte si vous vous êtes inscrit à AWS l'aide de l'option S'inscrire pour AWS (avancé) ou si vous avez

activé des fonctionnalités avancées pour votre compte. Pour comparer les options d'inscription, consultezComparez les options d'inscription.

L'activation de l'accès sécurisé pour la gestion du AWS compte permet à l'administrateur du compte de gestion de modifier les informations et les métadonnées (par exemple, les coordonnées principales ou secondaires) spécifiques à chaque compte de membre dans AWS Organizations. Pour plus d'informations, consultez la section Gestion du AWS compte et AWS Organizations dans 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 AWS Gestion du compte.

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

> **Autorisations minimales**
>
> Pour effectuer ces tâches, vous devez remplir les conditions suivantes :
>
> - Vous pouvez effectuer cette opération uniquement à partir du compte de gestion de l'organisation.
> - Toutes les fonctions doivent être activées pour votre organisation.

Console de gestion AWS

Pour activer un accès sécurisé pour AWS Gestion du compte

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Choisissez Services dans le volet de navigation.
3. Choisissez Gestion du AWS compte dans la liste des services.

4. Choisissez Enable trusted access (Activer l'accès approuvé).
5. Dans la boîte de dialogue Activer l'accès sécurisé pour la gestion des AWS comptes, tapez activer pour le confirmer, puis choisissez Activer l'accès sécurisé.

AWS CLI & SDKs

Pour activer un accès sécurisé pour AWS Gestion du compte

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 Account Management qui utilisent le `--accountId` paramètre pour référencer les comptes membres d'une organisation.

- AWS CLI : enable-aws-service-access

  L'exemple suivant active l'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 AWS Gestion du compte

Ces instructions expliquent comment activer un compte administrateur délégué pour la gestion des AWS comptes si vous vous êtes inscrit pour AWS utiliser Sign up for AWS (avancé) ou si vous avez activé des fonctionnalités avancées pour votre compte. Pour comparer les options d'inscription, consultezComparez les options d'inscription.

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

Pour enregistrer un compte de membre dans votre organisation en tant que compte d'administrateur délégué, procédez comme suit.

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 remplir les conditions suivantes :
>
> - Vous pouvez effectuer cette opération uniquement 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: administrateur délégué du registre

  L'exemple suivant enregistre un compte de 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 les opérations de gestion des comptes AWS CLI et de l'API SDK qui utilisent le `--account-id` paramètre pour référencer les comptes membres d'une organisation.

Console de gestion AWS

> Cette tâche n'est pas prise en charge dans la console de gestion des AWS comptes. Vous pouvez effectuer cette tâche uniquement à l'aide du AWS CLI ou d'une opération d'API provenant de l'un des AWS kits SDK.

Restreindre l'accès en utilisant AWS Organizations politiques de contrôle des services

Ces informations concernent la restriction de l'accès à l'aide de politiques de contrôle des AWS Organizations services si vous vous êtes inscrit pour AWS utiliser Sign up for AWS (avancé) ou si vous avez activé des fonctionnalités avancées pour votre compte. Pour comparer les options d'inscription, consultezComparez les options d'inscription.

Cette rubrique présente des exemples qui montrent comment vous pouvez utiliser les politiques de contrôle des services (SCP) AWS Organizations pour restreindre ce que peuvent faire les utilisateurs et les rôles des 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 de SCP
- Associer des SCP à des unités d'organisation et à des comptes
- Stratégies pour les SCP
- Syntaxe de la politique SCP

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

L'exemple suivant empêche les opérations d'`DeleteAlternateContact`API `PutAlternateContact` et d'être appelées par un compte membre en mode compte autonome. Cela empêche tout mandant des comptes concernés de modifier ses propres contacts alternatifs.

JSON

```
{
    "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 de membre de modifier des contacts alternatifs pour tout autre compte de membre de l'organisation

L'exemple suivant généralise l'`Resource`élément à « * », ce qui signifie qu'il s'applique à la fois aux demandes en mode autonome et aux demandes en mode organisation. 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.

JSON

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

Example Exemple 3 : Empêcher un compte de membre dans 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 unités d'organisation. Cela a pour effet d'empêcher un mandant de n'importe quel compte dans les unités d'organisation spécifiées de modifier ses propres contacts alternatifs.

Quand l'utiliser AWS Control Tower

Ces informations indiquent quand les utiliser AWS Control Tower si vous vous êtes inscrit pour AWS utiliser Sign up for AWS (avancé) ou si vous avez activé des fonctionnalités avancées pour votre compte. Pour comparer les options d'inscription, consultezComparez les options d'inscription.

AWS Organizations est le service de base qui vous permet de gérer et de sécuriser l'ensemble de votre AWS environnement de manière centralisée. 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 organisations, 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 proposée par AWS Control Tower étend les fonctionnalités de base de AWS Organizations. AWS Control Tower applique un ensemble de mesures préventives 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 avec 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 maintenant 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

Ces informations permettent de comprendre les modes de fonctionnement de l'API si vous vous êtes inscrit pour AWS utiliser Sign up for AWS (avancé) ou si vous avez activé des fonctionnalités avancées pour votre compte. Pour comparer les options d'inscription, consultezComparez les options d'inscription.

Les opérations d'API qui fonctionnent avec les attributs Compte AWS d'an 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 à un attribut de compte d'un autre compte membre de la même organisation ou le modifie. 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. Vous pouvez appeler les opérations dans ce mode uniquement à partir du compte de gestion de l'organisation ou du compte administrateur délégué pour la gestion des comptes.

Les opérations AWS CLI et le AWS SDK peuvent fonctionner dans un contexte autonome ou organisationnel.

- 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 l'opération fonctionne sur le compte des organisations spécifié.
  - Si le compte qui appelle l'opération est le compte de gestion ou le compte d'administrateur délégué pour le service de gestion des comptes, vous pouvez spécifier n'importe quel compte 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 qui inclut 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 qui inclut un `Resource` élément permettant d'`"*"`autoriser toutes les ressources ou un ARN qui utilise la syntaxe d'un compte 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 responsable IAM (utilisateur ou rôle), vous spécifiez les actions que ce responsable 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 de 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 auquel vous souhaitez faire référence est un compte autonome ou un compte appartenant à une organisation. Reportez-vous à 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'attributs de compte en mode autonome en n'incluant pas le `AccountID` paramètre.
  - Un ARN de compte pour un compte de membre d'une organisation :

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

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

Clés contextuelles pour les politiques IAM

Le service de gestion des comptes fournit également plusieurs clés de condition spécifiques au service de gestion des comptes qui permettent un contrôle précis des autorisations que vous accordez.

compte : AccountResourceOrgPaths

La clé contextuelle vous `account:AccountResourceOrgPaths` permet de spécifier un chemin dans la hiérarchie de votre organisation jusqu'à une unité organisationnelle (UO) spécifique. Seuls les comptes membres contenus dans cette unité d'organisation répondent à cette condition. L'extrait de code suivant limite la politique afin qu'elle ne s'applique qu'aux comptes appartenant à l'une des deux unités d'organisation spécifiées.

Comme il `account:AccountResourceOrgPaths` s'agit d'un type de chaîne à valeurs multiples, vous devez utiliser le `ForAnyValue` ou les opérateurs de chaîne `ForAllValues` à valeurs multiples. Notez également que le préfixe de la clé de condition est`account`, même si vous faites référence à des chemins vers des unités d'organisation dans une organisation.

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

compte : AccountResourceOrgTags

La clé contextuelle vous `account:AccountResourceOrgTags` permet de référencer les balises qui peuvent être associées à un compte dans une organisation. Une balise est une paire de key/value chaînes que vous pouvez utiliser pour classer et étiqueter les ressources de votre compte. Pour plus d'informations sur le balisage, voir Tag Editor dans le Guide de l'Groupes de ressources AWS utilisateur. Pour plus d'informations sur l'utilisation des balises dans le cadre d'une stratégie de contrôle d'accès basée sur les attributs, consultez la section À quoi sert ABAC AWS dans le guide de l'utilisateur IAM. L'extrait de code suivant limite la politique afin qu'elle ne s'applique qu'aux comptes d'une organisation qui ont la balise avec la clé `project` et une valeur égale à ou. `blue` `red`

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

Configurez votre Compte AWS

Ces instructions expliquent comment configurer votre compte Compte AWS si vous vous êtes inscrit pour AWS utiliser Sign up for AWS (avancé) ou si vous avez activé des fonctionnalités avancées pour votre compte. Pour comparer les options d'inscription, consultezComparez les options d'inscription.

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

> **Note**
>
> Si votre site Compte AWS a 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

- Créez un Compte AWS alias
- Activer ou désactiver Régions AWS dans votre compte
- Mettez à jour la facturation de votre Compte AWS
- Mettez à jour le Adresse e-mail de l'utilisateur racine
- Mettre à jour le mot de passe utilisateur root
- Mettez à jour votre Compte AWS name
- Mettez à jour les contacts alternatifs de votre Compte AWS

- Mettez à jour le contact principal de votre Compte AWS
- Afficher Compte AWS identifiants

Créez un Compte AWS alias

Ces instructions expliquent comment créer un Compte AWS alias si vous vous êtes inscrit pour AWS utiliser Sign up for AWS (advanced) ou si vous avez activé des fonctionnalités avancées pour votre compte. Pour comparer les options d'inscription, consultezComparez les options d'inscription.

Si vous souhaitez que l'URL de vos utilisateurs IAM contienne le nom de votre entreprise (ou un autre identifiant facile à retenir) 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.

Activer ou désactiver Régions AWS dans votre compte

Ces informations concernent l'activation ou la désactivation Régions AWS dans votre compte Compte AWS si vous vous êtes inscrit pour AWS utiliser Sign up for AWS (avancé) ou si vous avez activé des fonctionnalités avancées pour votre compte. Pour comparer les options d'inscription, consultezComparez les options d'inscription.

An Région AWS est un lieu physique dans le monde AWS doté de plusieurs zones de disponibilité. Les zones de disponibilité sont composées 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. L'exécution des charges de travail au Région AWS plus près des utilisateurs finaux peut améliorer les performances et réduire la latence. Pour une carte des régions disponibles et à venir, voir Régions et zones de disponibilité. Pour en savoir plus sur l'architecture de résilience de vos charges de travail Régions AWS et en savoir plus sur l'architecture de résilience adaptée à vos charges de travail, consultez la section Principes fondamentaux AWS relatifs à

Régions AWS se répartissent généralement en deux catégories de disponibilité pour les comptes :

- Régions par défaut : les régions lancées avant le 20 mars 2019 sont activées par défaut. Vous pouvez créer et gérer des ressources dans ces régions par défaut immédiatement après l'activation de votre compte. Les régions par défaut ne peuvent pas être activées ou désactivées.

- Opt-in Régions : les régions lancées après le 20 mars 2019 sont désactivées par défaut et sont appelées régions optionnelles. Les régions optionnelles désactivées ne sont pas affichées dans la barre de navigation de la console et vous ne pouvez pas utiliser ces régions pour créer des charges de travail tant qu'elles ne sont pas activées. Pour utiliser ces régions optionnelles, vous devez d'abord les activer dans votre Compte AWS. Après avoir activé une région optionnelle, vous pouvez sélectionner cette région dans la barre de navigation et créer et gérer des ressources dans cette région. Pour activer une région optionnelle pour vos comptes autonomes, voir Activer ou désactiver une région pour les comptes autonomes et pour activer une région optionnelle pour vos comptes membres, voir. Activer ou désactiver une région dans votre organisation

Lorsque vous vous inscrivez à un Compte AWS, vous AWS recommande une région optionnelle en fonction du pays de votre adresse de contact. Les clients d'un pays doté d'une AWS région d'adhésion voient une recommandation sur la page d'informations de contact leur demandant d'activer la région d'adhésion dans ce pays. Les clients résidant dans un pays comportant à la fois une région d'adhésion et une région par défaut, comme l'Inde, l'Australie ou le Canada, voient une recommandation les invitant à sélectionner la région d'adhésion si celle-ci est plus proche de chez eux que la région par défaut. Une fois qu'un compte est activé, vous pouvez activer d'autres régions AWS facultatives sur votre compte ou choisir de désactiver la région optionnelle que vous avez activée lors de votre inscription.

Lorsque vous créez une Compte AWS, vos données et informations d'identification IAM sont automatiquement configurées pour fonctionner dans toutes les régions par défaut, ce qui permet à l'utilisateur root et aux identités IAM disposant des autorisations appropriées d'accéder aux AWS services de ces régions à l'aide de leurs informations d'identification existantes. AWS Les régions opt-in sont désactivées par défaut, et les données et informations d'identification IAM ne sont pas initialement disponibles dans ces régions, ce qui empêche l'accès aux AWS services de cette région. Lorsque vous choisissez d'activer une région optionnelle, vos données IAM et AWS vos informations d'identification sont propagées à cette région. Une fois la propagation terminée et la région opt-in activée, l'utilisateur root et les identités IAM peuvent accéder aux AWS services de la région opt-in nouvellement activée en utilisant les mêmes informations d'identification IAM que celles utilisées dans les régions par défaut.

Lorsque vous désactivez une région optionnelle, vos informations d'identification IAM sont désactivées et vous perdez l'accès IAM aux ressources de cette région optionnelle. La désactivation d'une région optionnelle ne supprime pas les ressources de cette région et les frais liés aux ressources (le cas échéant) dans cette région optionnelle désactivée continuent de s'accumuler au taux standard.

> **Important**
>
> La désactivation d'une région désactive l'accès IAM aux ressources de la région. Cela ne supprime pas les ressources en question, qui continuent de générer des frais. Supprimez toutes les ressources restantes avant de désactiver une région.

AWS regroupe les régions en partitions. Chaque région se trouve dans exactement une partition, et chaque partition possède une ou plusieurs régions. Les partitions possèdent des instances indépendantes de Gestion des identités et des accès AWS (IAM) et fournissent une limite stricte entre les régions des différentes partitions. AWS Les régions commerciales se trouvent dans la `aws` partition, les régions de Chine sont dans la `aws-cn` partition et AWS GovCloud (US) les régions sont dans la `aws-us-gov` partition. En fonction de la partition sur laquelle vous avez créé votre Compte AWS, vous pouvez l'utiliser Régions AWS au sein de cette partition.

- Un compte en `aws` partition vous permet d'accéder à plusieurs régions de la partition commerciale afin que vous puissiez lancer AWS des ressources dans les emplacements qui répondent à vos besoins. Par exemple, vous souhaiterez peut-être lancer des instances Amazon EC2 en Europe pour vous rapprocher de vos clients européens ou pour répondre à des exigences légales.
- Un compte en `aws-us-gov` partition vous permet d'accéder à la AWS GovCloud (US-West) Région et à la AWS GovCloud (US-East) Région. Pour de plus amples informations, veuillez consulter AWS GovCloud (US).
- Un compte en `aws-cn` partition vous permet d'accéder aux régions de Pékin et du Ningxia uniquement. Pour plus d'informations, veuillez consulter Amazon Web Services en Chine.

Rubriques

- Référence de disponibilité régionale
- Considérations à prendre en compte avant d'activer et de désactiver les régions
- Délais de traitement et limites des demandes
- Activer ou désactiver une région pour les comptes autonomes
- Activer ou désactiver une région dans votre organisation

Référence de disponibilité régionale

Les tableaux suivants présentent une liste Régions AWS par type de disponibilité. Les régions par défaut sont activées automatiquement et ne peuvent pas être désactivées, tandis que les régions facultatives doivent être activées manuellement avant de pouvoir les utiliser :

Opt-in Regions

Les régions suivantes sont des régions facultatives qui doivent être activées avant de pouvoir les utiliser :

Nom	Code	Statut
Afrique (Le Cap)	`af-south-1`	GA
Asie-Pacifique (Hong Kong)	`ap-east-1`	GA
Asie-Pacifique (Taipei)	`ap-east-2`	GA
Asie-Pacifique (Hyderabad)	`ap-south-2`	GA
Asie-Pacifique (Jakarta)	`ap-southeast-3`	GA
Asie-Pacifique (Melbourne)	`ap-southeast-4`	GA
Asie-Pacifique (Malaisie)	`ap-southeast-5`	GA
Asie-Pacifique (Nouvelle Zélande)	`ap-southeast-6`	GA
Asie-Pacifique (Thaïlande)	`ap-southeast-7`	GA
Canada-Ouest (Calgary)	`ca-west-1`	GA
Europe (Zurich)	`eu-central-2`	GA
Europe (Milan)	`eu-south-1`	GA
Europe (Espagne)	`eu-south-2`	GA
Israël (Tel Aviv)	`il-central-1`	GA
Moyen-Orient (EAU)	`me-central-1`	GA

Nom	Code	Statut
Middle East (Bahrain)	me-south-1	GA
Mexique (Centre)	mx-central-1	GA

Default Regions

Les régions suivantes sont activées par défaut et ne peuvent pas être désactivées :

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
USA Est (Virginie du Nord)	us-east-1

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

Pour une liste des noms de régions et de leurs codes correspondants, voir Points de terminaison régionaux dans le Guide de référence AWS général. Pour une liste des AWS services pris en charge dans chaque région (sans 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) au lieu du point de terminaison global pour réduire la latence. Les jetons de session provenant de AWS STS points de terminaison régionaux sont valides dans toutes les AWS régions. Si vous utilisez des AWS STS points de terminaison régionaux, aucune modification n'est nécessaire. Toutefois, les jetons de session provenant du point de AWS STS terminaison global (https://sts.amazonaws.com) ne sont valides Régions AWS que s'ils sont activés par défaut 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 global pour émettre des jetons de session valides pour tous Régions AWS. Les jetons de session valides dans toutes les régions sont plus volumineux. Si vous stockez des jetons de session, ces jetons plus volumineux peuvent affecter vos systèmes. Pour plus d'informations sur la façon dont les AWS STS points de terminaison fonctionnent avec AWS les régions, consultez la section Gestion AWS STS dans une AWS région.

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 :

- Vous pouvez utiliser toutes les régions de destination dans une zone géographique d'inférence interrégionale, quel que soit leur Region-opt statut. Certains services d'IA AWS générative,

notamment Amazon Bedrock (voir Augmenter le débit grâce à l'inférence interrégionale) et Amazon Q Developer (voir le Cross-region traitement dans Amazon Q Developer) utilisent l'inférence interrégionale. Si vous utilisez ces services, ils sélectionnent automatiquement les meilleures, 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 la disponibilité des calculs et des modèles disponibles.

- Vous pouvez utiliser les autorisations IAM pour contrôler l'accès aux régions : Gestion des identités et des accès AWS (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 touche de `aws:RequestedRegion` condition pour contrôler l'accès Services AWS à un Région AWS.
- L'activation et la désactivation d'une région sont gratuites. L'activation ou la désactivation d'une région sont gratuites. Seules les ressources que vous créez dans la nouvelle région vous sont facturées.
- EventBridge Intégration à Amazon : vous pouvez vous abonner aux notifications de mise à jour du statut par région dans. EventBridge Une EventBridge notification sera créée pour chaque changement de statut, permettant aux clients d'automatiser les flux de travail.
- Region-opt État expressif : en raison de la nature asynchrone d' enabling/disabling une région d'adhésion, il existe quatre statuts potentiels pour une demande d'option de région :
  - `ENABLING`
  - `DISABLING`
  - `ENABLED`
  - `DISABLED`

  Vous ne pouvez pas annuler une inscription ou une désinscription lorsqu'elle est en cours `ENABLING` ou non`DISABLING`. Dans le cas contraire, un `ConflictException` sera lancé. Une demande d'option de région terminée (Enabled/Disabled) 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`.

Délais de traitement et limites des demandes

Lorsque vous activez ou désactivez des régions, tenez compte des limites de temps et de requêtes suivantes :

- L'activation d'une région prend de quelques minutes à plusieurs heures dans certains cas. Lorsque vous activez une région, AWS effectue des actions pour préparer votre compte dans cette région, par exemple en distribuant vos ressources IAM à 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.
- La désactivation d'une région n'est pas toujours visible immédiatement : 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.
- 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 particulière pour un compte.
- Les organisations peuvent avoir 50 demandes d'option de 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 correspond à l'activation ou à la désactivation d'une région particulière pour un compte.

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 Console de gestion AWS procédure suivante ne fonctionne toujours que dans le contexte autonome. Vous pouvez utiliser le Console de gestion AWS pour afficher ou mettre à jour uniquement les régions disponibles dans le compte que vous avez utilisé pour lancer l'opération.

Console de gestion AWS

Pour activer ou désactiver une région pour une application autonome Compte AWS

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

1. Connectez-vous en Console de gestion AWS tant 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 choisissez Compte.
3. Sur la page Compte, faites défiler la page vers le bas jusqu'à la section Régions AWS.
4. Choisissez la région que vous souhaitez activer ou désactiver, puis choisissez l'action souhaitée Activer ou Désactiver. Vous serez invité à confirmer.
5. Si vous avez choisi l'option Activer, vérifiez le texte affiché, puis choisissez Activer la région.

   Si vous avez choisi l'option Désactiver, vérifiez le texte affiché, tapez **`disable`** pour confirmer, puis choisissez Désactiver la région.

   Une fois la région optionnelle activée, vous pouvez sélectionner cette région dans la barre de navigation de la région. Pour savoir comment sélectionner une région, voir Choisir une région dans la barre de navigation du Console de gestion AWS et pour les paramètres de console spécifiques à une région dans votre compte, voir Configuration de la région par défaut dans le Console de gestion AWS.

AWS CLI & SDKs

Vous pouvez activer, désactiver, lire et répertorier le statut d'activation d'une région à l'aide des AWS CLI commandes suivantes ou de leurs opérations équivalentes dans le AWS SDK :

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

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

- `account:ListRegions`

Si vous utilisez ces autorisations individuelles, vous pouvez accorder à certains utilisateurs la possibilité de lire uniquement les informations relatives à la sélection d'une région et autoriser d'autres utilisateurs à lire et à écrire.

L'exemple suivant active une région 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 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 état 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 les comptes de vos membres AWS Organizations, suivez les étapes de la procédure suivante.

> **Note**
>
> Les politiques AWS Organizations gérées `AWSOrganizationsFullAccess` sont `AWSOrganizationsReadOnlyAccess` ou sont mises à jour pour autoriser l'accès aux API de gestion des AWS comptes afin que vous puissiez accéder aux données du compte depuis

la AWS Organizations console. Pour consulter les politiques gérées mises à jour, voir Mises à jour des politiques AWS gérées des organisations.

> **Note**
>
> Avant de pouvoir effectuer ces opérations à partir du compte de gestion ou d'un compte d'administrateur délégué dans 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 lors de la création de votre organisation. Si votre organisation est configurée pour la facturation consolidée uniquement et que vous souhaitez activer toutes les fonctionnalités, consultez Activation de toutes les fonctionnalités dans votre organisation.
> - Activez un accès sécurisé pour le service de gestion des AWS comptes. Pour configurer cela, consultezActivez un accès sécurisé pour AWS Gestion du compte.

Console de gestion AWS

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 AWS page, 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 choisissez l'option Activer ou Désactiver.
6. Si vous avez choisi l'option Activer, vérifiez le texte affiché, puis choisissez Activer la région.
7. Si vous avez choisi l'option Désactiver, vérifiez le texte affiché, tapez Désactiver pour confirmer, puis choisissez Désactiver la région.

AWS CLI & SDKs

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

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

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

Si vous utilisez ces autorisations individuelles, vous pouvez accorder à certains utilisateurs la possibilité de lire uniquement les informations relatives à la sélection d'une région et autoriser d'autres utilisateurs à lire et à écrire.

L'exemple suivant active une région 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 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. Dans le cas contraire, vous recevrez un`TooManyRequestsException`.

L'opération est asynchrone. La commande suivante vous permettra de voir le dernier état 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

Ces instructions expliquent comment mettre à jour votre facturation Compte AWS si vous vous êtes inscrit pour AWS utiliser Sign up for AWS (avancé) ou si vous avez activé des fonctionnalités avancées pour votre compte. Pour comparer les options d'inscription, consultezComparez les options d'inscription.

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

Mettez à jour le Adresse e-mail de l'utilisateur racine

Ces instructions expliquent comment mettre à jour l'adresse e-mail de l'utilisateur root si vous vous êtes inscrit à AWS l'aide de l'option Inscription pour AWS (avancée) ou si vous avez activé les fonctionnalités avancées de votre compte. Pour comparer les options d'inscription, voirComparez les options d'inscription.

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 :

- Comptes autonomes Comptes AWS ou de gestion : si vous n'êtes Comptes AWS pas associé à une organisation, ou pour le compte de gestion d'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 un compte autonome Compte AWS ou de gestion.
- 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'adresse e-mail de l'utilisateur root associée au compte membre depuis la AWS Organizations console ou par programmation via la AWS CLI et les SDK. 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

- Mettez à jour le e-mail de l'utilisateur root pour un appareil autonome Compte AWS ou compte de gestion
- Mettez à jour le e-mail de l'utilisateur root pour tous Compte AWS dans votre organisation

Mettez à jour le e-mail de l'utilisateur root pour un appareil autonome Compte AWS ou compte de gestion

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

Console de gestion AWS

> **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 Console de gestion AWStant 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 SDK. Vous ne pouvez effectuer cette tâche qu'à l'aide du Console de gestion AWS.

Mettez à jour le e-mail de l'utilisateur root pour tous Compte AWS dans 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 Console de gestion AWS après vous être connecté en tant qu'utilisateur root. Pour obtenir des instructions détaillées, suivez les étapes indiquées dansMettez à jour le e-mail de l'utilisateur root pour un appareil autonome Compte AWS ou compte de gestion.

> **Note**
>
> Vous ne pouvez pas mettre à jour l'adresse e-mail de l'utilisateur root d'un compte de projet, qui est un compte de membre que vous avez créé en tant que projet dans AWS les paramètres. Un AWS Builder ID est propriétaire de chaque compte de projet au lieu de l'adresse e-mail de l'utilisateur root, et cela ne change pas lorsque vous activez les fonctionnalités avancées. Pour plus d'informations, consultez Comptes de projet après avoir activé les fonctionnalités avancées.

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 le Adresse e-mail de l'utilisateur racine pour un compte de membre utilisant le 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 racine (non 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 autre organisation que celle que vous utilisez pour appeler l'opération.
- Pour un compte de projet, `StartPrimaryEmailUpdate` et `AcceptPrimaryEmailUpdate` échouez avec une `AccessDeniedException` erreur même si vous disposez des autorisations requises.

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 les API de messagerie principales ensemble dans l'ordre indiqué dans les exemples suivants.

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

Ces instructions expliquent comment mettre à jour le mot de passe de l'utilisateur root si vous vous êtes inscrit pour AWS utiliser Sign up for AWS (avancé) ou si vous avez activé des fonctionnalités avancées pour votre compte. Pour comparer les options d'inscription, consultezComparez les options d'inscription.

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

Console de gestion AWS

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 Console de gestion AWS tant que 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, remplissez 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, y compris les meilleures pratiques pour définir les mots de passe des utilisateurs root, consultez la section Modifier le mot de passe correspondant Utilisateur racine d'un compte AWS dans le 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 depuis l'un des AWS kits SDK. Vous pouvez effectuer cette tâche uniquement à l'aide du Console de gestion AWS.

Mettez à jour votre Compte AWS name

Ces instructions expliquent comment mettre à jour votre Compte AWS nom si vous vous êtes inscrit pour AWS utiliser Sign up for AWS (avancé) ou si vous avez activé des fonctionnalités avancées pour votre compte. Pour comparer les options d'inscription, consultezComparez les options d'inscription.

Lorsque vous gérez plusieurs unités Comptes AWS, utilisez des conventions de dénomination claires, adaptées aux unités commerciales et aux applications d'identification et d'organisation. Lors de réorganisations, de fusions, d'acquisitions ou de mises à jour de conventions de dénomination, vous devrez peut-être renommer les comptes pour maintenir des normes d'identification et administratives cohérentes.

Le nom d'un compte apparaît à plusieurs endroits, par exemple sur votre facture et sur des consoles telles que le tableau de bord de facturation et de gestion des coûts et la AWS Organizations console. Nous vous recommandons d'utiliser une méthode standard pour nommer vos comptes afin que les noms de vos comptes 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 - produit). Pour des raisons de confidentialité et de sécurité, évitez d'utiliser des noms de compte qui contiennent des informations personnelles identifiables (PII).

- Comptes autonomes Comptes AWS ou de gestion : pour les comptes Comptes AWS non associés à une organisation, ou pour le compte de gestion d'une organisation, vous pouvez mettre à jour le nom de votre compte à l'aide des kits de développement logiciel (SDK) ou des Console de gestion AWS kits de développement logiciel (SDK). AWS CLI Pour savoir comment procéder, consultez Mettez à jour le nom de votre compte pour un compte autonome Compte AWS ou compte de gestion.
- Comptes AWS au sein d'une organisation : pour les comptes membres qui font partie d'un compte de gestion ou d'un compte administrateur délégué AWS Organizations, un utilisateur peut mettre à jour de manière centralisée le nom de compte de tout compte membre de l'organisation depuis la AWS Organizations console ou par programmation via les SDK AWS CLI et. Pour savoir comment procéder, consultez Mettez à jour le nom de votre compte pour tout Compte AWS au sein de votre organisation.

> **Note**
>
> Les modifications apportées à un 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 ou compte de gestion

- Mettez à jour le nom de votre compte pour tout Compte AWS au sein de votre organisation

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

Pour modifier le nom d'un compte autonome Compte AWS ou d'un compte de gestion, effectuez les étapes de la procédure suivante.

Console de gestion AWS

> **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 requise pour mettre à jour le nom d'un compte. Lorsque vous utilisez un utilisateur IAM ou un rôle IAM, vous devez disposer au moins des autorisations IAM suivantes :
>
> - `account:GetAccountInformation`
> - `account:PutAccountName`

Pour mettre à jour le nom d'un compte autonome ou d'un compte de gestion

1. Utilisez votre Compte AWS adresse e-mail et votre mot de passe pour vous connecter en Console de gestion AWS tant que 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 du 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 IAM ou votre rôle IAM doit disposer au moins des autorisations IAM suivantes :
>
> - `account:GetAccountInformation`
> - `account:PutAccountName`

Pour mettre à jour le nom d'un compte autonome ou d'un compte de gestion

Vous pouvez effectuer l'une des opérations suivantes :

- AWS CLI: nom-du-compte

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

- AWS SDK : PutAccountName

Mettez à jour le nom de votre compte pour tout Compte AWS au sein de votre organisation

En AWS Organizations mode Toutes fonctionnalités, les utilisateurs IAM autorisés ou les rôles IAM dans les comptes de gestion et les comptes d'administrateur délégué peuvent gérer les noms de compte de manière centralisée.

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

Exigences

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 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 lors de la création de votre organisation. Si votre organisation est configurée pour la facturation consolidée uniquement et que vous souhaitez activer toutes les fonctionnalités, consultez Activation de toutes les fonctionnalités pour une organisation.
- Vous devez activer un accès sécurisé pour le service de gestion des AWS comptes. Pour configurer cela, consultezActivez un accès sécurisé pour AWS Gestion du compte.

Console de gestion AWS

> **Autorisations minimales**
>
> Pour mettre à jour le nom d'un compte de 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 volet de navigation principal, sélectionnez Comptes AWS.
3. Sur la Comptes AWS page, choisissez le compte de 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 de 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 effectuer l'une des opérations suivantes :

- AWS CLI: nom-du-compte

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

- AWS SDK : PutAccountName

Mettez à jour les contacts alternatifs de votre Compte AWS

Ces instructions expliquent comment mettre à jour vos contacts alternatifs Compte AWS si vous vous êtes inscrit AWS via Sign up for AWS (avancé) ou si vous avez activé des fonctionnalités avancées pour votre compte. Pour comparer les options d'inscription, consultezComparez les options d'inscription.

Les contacts alternatifs AWS permettent de contacter jusqu'à trois contacts alternatifs 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 racine.

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

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

Vous pouvez ajouter ou modifier d'autres contacts 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

l' AWS interface de ligne de commande et les kits de développement logiciel. Pour savoir comment procéder, voir Mettre à jour les contacts alternatifs pour un contact autonome Compte AWS.

- Comptes AWS au sein d'une organisation : pour les comptes membres qui font partie d'une AWS organisation, un utilisateur du compte de gestion ou du compte administrateur délégué peut mettre à jour de manière centralisée n'importe quel compte membre de l'organisation depuis la AWS Organizations console ou par programmation via la AWS CLI et les SDK. Pour savoir comment procéder, voir Mettre à jour les contacts alternatifs pour tous les membres Compte AWS de votre organisation.

Rubriques

- Exigences relatives au numéro de téléphone et à l'adresse e-mail
- Mettre à jour les contacts alternatifs pour un contact autonome Compte AWS
- Mettez à jour les contacts alternatifs pour tous Compte AWS dans 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 coordonnées secondaires de votre compte, nous vous recommandons de vérifier les exigences suivantes lorsque vous saisissez 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 alternatifs pour un contact autonome Compte AWS

Pour ajouter ou modifier les contacts alternatifs pour un contact autonome Compte AWS, effectuez les étapes de la procédure suivante. La Console de gestion AWS procédure suivante ne fonctionne toujours que dans le contexte autonome. Vous pouvez utiliser le Console de gestion AWS pour accéder ou modifier uniquement les contacts alternatifs du compte que vous avez utilisé pour appeler l'opération.

Console de gestion AWS

Pour ajouter ou modifier les contacts alternatifs pour un compte 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 Console de gestion AWS tant qu'utilisateur ou rôle IAM disposant des autorisations minimales.
2. Choisissez le nom de votre compte en haut à droite de la fenêtre, puis choisissez Compte.
3. Sur la page Compte, faites défiler la page jusqu'à Contacts alternatifs, 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 précédemment.

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

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

5. Après avoir effectué toutes 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 d'administrateur délégué dans 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 et autoriser d'autres à lire et à écrire.

Example

L'exemple suivant récupère 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 chargé 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, la première 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 alternatif de 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 pour tous Compte AWS dans votre organisation

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

Exigences

Pour mettre à jour des contacts alternatifs avec la AWS Organizations console, vous devez effectuer certains réglages 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 lors de la création de votre organisation. Si votre organisation est configurée pour la facturation consolidée uniquement et que vous souhaitez activer toutes les fonctionnalités, consultez Activation de toutes les fonctionnalités pour une organisation.
- Vous devez activer un accès sécurisé pour le service de gestion des AWS comptes. Pour configurer cela, consultezActivez un accès sécurisé pour AWS Gestion du compte.

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

Console de gestion AWS

Pour ajouter ou modifier les contacts alternatifs pour n'importe quel Compte AWS dans votre organisation

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

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

6. Après avoir effectué toutes 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 d'administrateur délégué dans 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 et autoriser d'autres à lire et à écrire.

Example

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

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

Example

L'exemple suivant définit le contact alternatif chargé des opérations 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 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, la première 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 alternatif de sécurité 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 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 contextuelle `account:AlternateContactTypes` pour spécifier lequel des trois types de contact est autorisé (ou refusé) par la politique IAM. Par exemple, l'exemple de politique d'autorisation IAM suivant utilise cette clé de condition pour permettre aux responsables connectés de récupérer, mais pas de modifier, uniquement le contact `BILLING` alternatif associé à un compte spécifique au sein d'une organisation.

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

Mettez à jour le contact principal de votre Compte AWS

Ces instructions indiquent comment mettre à jour le contact principal de votre compte Compte AWS si vous vous êtes inscrit à AWS l'aide de l'option S'inscrire à AWS (avancé) ou si vous avez activé les fonctionnalités avancées de votre compte. Pour comparer les options d'inscription, voirComparez les options d'inscription.

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 pouvez également vérifier le numéro de téléphone du contact principal. Pour plus d'informations, consultez Vérifiez le numéro de téléphone du contact principal.

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

- Autonome Comptes AWS : si vous n'êtes Comptes AWS pas associé à une organisation, vous pouvez mettre à jour le contact principal de votre compte à l'aide de la console AWS de gestion

ou via la AWS CLI et les SDK. Pour savoir comment procéder, voir Mettre à jour le contact Compte AWS principal autonome.

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

Rubriques

- Exigences relatives au numéro de téléphone et à l'adresse e-mail
- Mettre à jour le contact principal pour un contact autonome Compte AWS ou compte de gestion
- Mettez à jour le contact principal pour n'importe quel AWS compte de membre dans votre organisation
- Vérifiez le numéro de téléphone du contact principal

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 (US/Canada) ou +44 (UK).
- Les numéros de téléphone ne doivent pas inclure d'espaces entre le code 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 ou compte de gestion

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

Console de gestion AWS

Pour modifier votre contact principal en tant que contact autonome Compte AWS ou compte de gestion

> **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 Console de gestion AWStant 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. Après avoir effectué toutes les modifications, choisissez Mettre à jour.

AWS CLI & SDKs

Vous pouvez récupérer, mettre à jour ou supprimer les informations de contact 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 pour n'importe quel AWS compte de membre dans votre organisation

Pour modifier vos coordonnées principales dans n'importe quel compte AWS 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, voirActivez un accès sécurisé pour AWS Gestion du compte.

Console de gestion AWS

Pour modifier votre contact principal pour n'importe quel Compte AWS dans 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. Après avoir effectué toutes les modifications, choisissez Enregistrer.

Si vous modifiez le numéro de téléphone, nous envoyons un code de vérification au nouveau numéro lorsque vous sélectionnez Enregistrer. Vous pouvez vérifier le numéro immédiatement ou ultérieurement. Pour plus d'informations, consultez Vérifiez le numéro de téléphone d'un compte membre de votre organisation.

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.

Vérifiez le numéro de téléphone du contact principal

Vous pouvez vérifier le numéro de téléphone figurant dans les informations de contact principales d'un Compte AWS. La vérification confirme que le numéro de téléphone enregistré peut recevoir des SMS de notre part.

Lorsque vous lancez la vérification, nous envoyons un code de vérification à 6 chiffres par SMS au numéro de téléphone actuellement enregistré pour le compte. Vous ne saisissez pas de numéro de téléphone pour démarrer la vérification. Pour terminer, saisissez le code avant son expiration.

Tenez compte des points suivants lorsque vous vérifiez un numéro de téléphone :

- Le code expire 5 minutes après son envoi.
- Si vous demandez un nouveau code, les codes que nous avons envoyés précédemment ne fonctionnent plus.
- Si le code est incorrect ou a expiré, demandez un nouveau code et réessayez.
- Si le numéro de téléphone change après l'envoi d'un code, vous ne pouvez pas utiliser ce code. Demandez un nouveau code pour le numéro actuel.
- Le statut de vérification décrit toujours le numéro de téléphone actuellement enregistré. Si vous modifiez le numéro de téléphone, le statut décrit le nouveau numéro.
- Pour un compte membre au sein d'une organisation, le code est attribué au numéro de téléphone principal du compte membre, et non au vôtre. Avant de commencer, assurez-vous de pouvoir obtenir le code auprès de la personne qui possède ce téléphone.

Pour vérifier l'état de la vérification, utilisez l'GetContactInformationopération. Le `VerificationStatus` champ de la réponse contient l'une des valeurs suivantes :

- `VERIFIED`— Le numéro de téléphone enregistré est vérifié.
- `UNVERIFIED`— Le numéro de téléphone enregistré n'est pas vérifié.
- `NOT_SUPPORTED`— La vérification du numéro de téléphone n'est pas disponible pour ce compte.

Vérifiez le numéro de téléphone d'un service autonome ou de gestion Compte AWS

Pour vérifier le numéro de téléphone du compte dont vous utilisez les informations d'identification, utilisez les AWS CLI commandes suivantes ou leurs opérations équivalentes au AWS SDK :

- SendPhoneNumberVerification
- VerifyPhoneNumber

> **Autorisations minimales**
>
> Pour chaque opération, vous devez disposer de l'autorisation correspondant à cette opération :
>
> - `account:SendPhoneNumberVerification`
> - `account:VerifyPhoneNumber`
>
> Pour vérifier l'état de la vérification, vous devez également`account:GetContactInformation`.

Example

L' AWS CLI exemple suivant envoie un code de vérification au numéro de téléphone du contact principal du compte de l'appelant :

```
$ aws account send-phone-number-verification
{
    "Status": "PENDING"
}
```

Example

L' AWS CLI exemple suivant envoie le code pour terminer la vérification :

```
$ aws account verify-phone-number --otp 123456
{
    "Status": "VERIFIED"
}
```

Example

L' AWS CLI exemple suivant permet de récupérer le statut de vérification du numéro de téléphone principal de l'appelant :

```
$ aws account get-contact-information --query VerificationStatus
"VERIFIED"
```

Vérifiez le numéro de téléphone d'un compte membre de votre organisation

Vous pouvez vérifier le numéro de téléphone d'un compte membre à l'aide de la AWS Organizations console AWS CLI, du ou d'un AWS SDK. Avant de commencer, suivez les étapes décrites dansExigences supplémentaires.

Console de gestion AWS

Pour vérifier le numéro de téléphone principal d'un compte membre

Autorisations minimales

Pour effectuer les étapes suivantes, vous devez au moins disposer des autorisations IAM suivantes :

- `account:GetContactInformation`(pour voir le numéro de téléphone et s'il est vérifié)
- `account:SendPhoneNumberVerification`(pour envoyer un code de vérification)
- `account:VerifyPhoneNumber`(pour soumettre le code)

La politique `AWSOrganizationsFullAccess` gérée n'inclut pas `account:SendPhoneNumberVerification` ou`account:VerifyPhoneNumber`. Si vous vous fiez à cette politique, accordez ces autorisations séparément.

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 membre.
3. Choisissez Informations de contact, puis localisez le contact principal.
4. Si le numéro de téléphone n'est pas vérifié, il apparaît avec un avertissement. Choisissez le numéro de téléphone, puis sélectionnez Vérifier le numéro de téléphone. Nous envoyons un code à 6 chiffres au numéro de téléphone du compte membre.
5. Entrez le code dans le champ Code de vérification, puis choisissez Vérifier.

   Si le code n'arrive pas, choisissez Renvoyer le code lorsque cette option sera disponible.

AWS CLI & SDKs

Pour vérifier le numéro de téléphone d'un compte membre, utilisez les AWS CLI commandes suivantes ou leurs opérations équivalentes au AWS SDK, et spécifiez l'ID du compte membre :

- SendPhoneNumberVerification
- VerifyPhoneNumber

Remarques

- Les informations d'identification que vous utilisez doivent provenir du compte de gestion de l'organisation ou du compte administrateur délégué pour la gestion des AWS 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:SendPhoneNumberVerification`
- `account:VerifyPhoneNumber`

Pour vérifier l'état de la vérification, vous devez également`account:GetContactInformation`.

Example

L' AWS CLI exemple suivant envoie un code de vérification au numéro de téléphone du contact principal du compte membre spécifié :

```
$ aws account send-phone-number-verification --account-id 123456789012
{
    "Status": "PENDING"
}
```

Example

L' AWS CLI exemple suivant envoie le code que nous avons envoyé au numéro de téléphone du compte du membre :

```
$ aws account verify-phone-number --account-id 123456789012 --otp 123456
{
    "Status": "VERIFIED"
}
```

Afficher Compte AWS identifiants

Ces informations concernent l'affichage Compte AWS des identifiants si vous vous êtes inscrit pour AWS utiliser Sign up for AWS (avancé) ou si vous avez activé des fonctionnalités avancées pour votre compte. Pour comparer les options d'inscription, consultezComparez les options d'inscription.

AWS attribue les identifiants uniques suivants à chacun d'entre eux : 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 leurs Amazon Resource Names (ARN). La partie ID de compte permet de distinguer les ressources d'un compte des ressources d'un autre compte. Si vous êtes un utilisateur Gestion des identités et des accès AWS (IAM), vous pouvez vous connecter à l' Console de gestion AWS aide de l'ID de compte ou de l'alias du compte. Bien que les identifiants de compte, comme toute information d'identification, doivent être utilisés et partagés avec soin, ils ne sont pas considérés comme des informations secrètes, sensibles ou confidentielles.

ID utilisateur canonique

Un identifiant alphanumérique, tel que`79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be`, qui est une forme masquée de l'identifiant. Compte AWS Vous pouvez utiliser cet identifiant pour identifier et autoriser l'accès entre comptes à des compartiments et à des objets à l'aide d'Amazon Simple Storage Service (Amazon S3). Compte AWS Vous pouvez récupérer l'ID utilisateur canonique qui vous correspond Compte AWS en tant qu'utilisateur root ou utilisateur IAM.

Vous devez être authentifié AWS pour voir ces identifiants.

> **Warning**
>
> Ne communiquez pas vos AWS informations d'identification (y compris vos mots de passe et vos 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 Compte AWS que vous.

Trouvez votre Compte AWS ID

Vous pouvez trouver l' Compte AWS ID à l'aide du Console de gestion AWS ou du 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'ID de compte est le même que vous soyez connecté en tant qu'utilisateur root ou en tant qu'utilisateur IAM.

Trouver l'identifiant de votre compte en tant qu'utilisateur root

Console de gestion AWS

Pour trouver votre Compte AWS ID lors de la connexion 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 choisissez Informations de sécurité.

   > **Tip**
   >
   > Si l'option Identifiants de sécurité n'apparaît pas, 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 l'entrée Compte 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 identifiant.

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 l'identifiant de votre compte en tant qu'utilisateur IAM

Console de gestion AWS

Pour trouver votre Compte AWS ID lors de la connexion 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 choisissez Informations de sécurité.

   > **Tip**
   >
   > Si l'option Identifiants de sécurité n'apparaît pas, 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 l'entrée Compte 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 l'Compte AWS identifiant.

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 le nom d'utilisateur canonique de votre Compte AWS

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

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

Console de gestion AWS

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 disposer des éléments suivants :
  - `account:GetAccountInformation`

1. Connectez-vous en Console de gestion AWS tant qu'utilisateur root ou utilisateur IAM.
2. Dans la barre de navigation en haut à droite, choisissez le nom ou le numéro de votre compte, puis choisissez Informations de sécurité.

> **Tip**
>
> Si l'option Identifiants de sécurité n'apparaît pas, 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 l'entrée Compte et le numéro d'identification du compte à côté.

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

AWS CLI & SDKs

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

La même commande AWS CLI d'API fonctionne pour les Utilisateur racine d'un compte 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 avec un rôle IAM

Console de gestion AWS

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

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

1. Connectez-vous en Console de gestion AWS tant qu'utilisateur fédéré avec 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, votre identifiant canonique 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
```

Résolvez vos problèmes Compte AWS

Ces informations visent à résoudre votre problème Compte AWS si vous vous êtes inscrit pour AWS utiliser Sign up for AWS (avancé) ou si vous avez activé des fonctionnalités avancées pour votre compte. Pour comparer les options d'inscription, consultezComparez les options d'inscription.

Utilisez les informations des 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'AWS Sign-In utilisateur.

Résolution des problèmes liés aux rubriques

- Résolution des problèmes liés à Compte AWS création
- Résolution des problèmes liés à Compte AWS fermeture
- Résolution d'autres problèmes liés à Comptes AWS

Résolution des problèmes liés à Compte AWS création

Ces informations concernent la résolution des problèmes liés à Compte AWS la création si vous vous êtes inscrit pour AWS utiliser Sign up for AWS (avancé) ou si vous avez activé des fonctionnalités avancées pour votre compte. Pour comparer les options d'inscription, consultezComparez les options d'inscription.

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	Inscrivez-vous pour AWS (avancé)	Ce guide
Que dois-je faire si je n'ai pas reçu d'appel AWS pour vérifier 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

Problème	Lien de référence	Source
Comment puis-je résoudre l'erreur « nombre maximum de tentatives échouées » lorsque j'essaie de vérifier mon identité Compte AWS par téléphone ?	https://repost.aws/knowledge-center/maximum-failed-attempts	AWS re:Post
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 Sign-In Guide de l'utilisateur

Pour obtenir de l'aide supplémentaire, nous vous recommandons de AWS re:Post rechercher du contenu lié à votre problème spécifique. Si vous avez toujours besoin d'aide, contactez AWS Support.

Résolution des problèmes liés à Compte AWS fermeture

Ces informations concernent la résolution des problèmes liés à Compte AWS la fermeture si vous vous êtes inscrit pour AWS utiliser Sign up for AWS (avancé) ou si vous avez activé des fonctionnalités avancées pour votre compte. Pour comparer les options d'inscription, consultezComparez les options d'inscription.

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 des informations générales sur le processus de fermeture de 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_EXCEEDED » 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 figurant 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 Console de gestion AWS tant qu'utilisateur root pour fermer votre compte. Si vous ne parvenez pas à vous connecter, consultez 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 envoyé uniquement à l'adresse e-mail de l'utilisateur root. Adresse e-mail pour le Compte AWS. Si vous ne recevez pas cet e-mail dans les heures qui suivent, vous pouvez vous connecter en Console de gestion AWS tant qu'utilisateur root pour vérifier que votre compte est fermé. Si votre compte a été clôturé avec succès, vous verrez s'afficher un message indiquant que votre compte est fermé. Si le compte que vous avez fermé est un compte de membre, vous pouvez vérifier que la fermeture a bien été effectuée en vérifiant si le compte fermé est étiqueté comme `CLOSED` 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 de confirmation par e-mail 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 n'y a plus de comptes de membres actifs dans votre organisation, accédez à la AWS Organizations console et assurez-vous que les comptes de tous les membres apparaissent à `Closed` côté de leur nom de compte. Après cela, 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 Console de gestion

AWS 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_EXCEEDED » lorsque j'essaie de fermer un compte membre

Vous ne pouvez fermer que 20 % des comptes de membres sur une période de 30 jours consécutifs. Ce quota n'est pas lié au mois civil, mais commence lorsque vous fermez un compte. Dans les 30 jours suivant la fermeture initiale de votre compte, vous ne pouvez pas dépasser la limite de 20 %. La fermeture minimale du compte est de 250 et la fermeture maximale du compte est de 1 000, même si 20 % des comptes dépassent 1 000. Pour plus d'informations sur les quotas des organisations, consultez la section Quotas pour AWS Organizations dans le Guide de AWS Organizations l'utilisateur.

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 de membre actif. Pour vérifier qu'il n'y a plus de comptes de membres actifs dans votre organisation, accédez à la AWS Organizations console et assurez-vous que les comptes de tous les membres apparaissent à `Closed` côté de leur nom de compte. Après cela, vous pouvez fermer le compte de gestion.

Résolution d'autres problèmes liés à Comptes AWS

Ces informations concernent la résolution d'autres problèmes liés à votre compte Compte AWS si vous vous êtes inscrit à AWS l'aide de l'option Inscription à AWS (avancée) ou si vous avez activé les fonctionnalités avancées de votre compte. Pour comparer les options d'inscription, voirComparez les options d'inscription.

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 un cas de fraude Compte AWS activity
- J'ai besoin de fermer mon Compte AWS

- Je reçois un AccessDeniedExceptionlorsque je mets à jour l'adresse e-mail d'un utilisateur root

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 a mis en place des protections qui vous obligent à prouver que vous êtes le titulaire 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 un cas de fraude Compte AWS activity

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

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

J'ai besoin de fermer mon Compte AWS

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

Je reçois un **`AccessDeniedException`**lorsque je mets à jour l'adresse e-mail d'un utilisateur root

Si le compte membre est un compte de projet, vous ne pouvez pas mettre à jour son adresse e-mail d'utilisateur root. Un AWS Builder ID est propriétaire de chaque compte de projet au lieu de l'adresse e-mail de l'utilisateur root. Pour plus d'informations, consultez Comptes de projet après avoir activé les fonctionnalités avancées.

Gérer des comptes en Inde

Ces informations concernent la gestion des comptes en Inde si vous vous êtes inscrit à AWS l'aide de l'option S'inscrire AWS pour (avancé) ou si vous avez activé les fonctionnalités avancées de votre compte. Pour comparer les options d'inscription, voirComparez les options d'inscription.

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 Compte AWS avec AWS Inde
- Gérez les informations de vérification de vos clients

Créez un Compte AWS avec AWS 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 vous inscrire à un AWS Compte 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 informations de contact 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 choisissez 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 plus d'informations, consultez 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), AWS elle 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' India-based adresse 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.

Si votre compte de gestion a activé l'héritage par validation client, le statut de vérification de votre compte reflète le statut de ce compte. Vous n'avez aucune action à effectuer lorsque l'héritage est actif.

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 Console de gestion AWS.
2. Dans la barre de navigation, dans le coin supérieur droit, choisissez le nom de votre compte (ou alias), puis cliquez sur 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 Soumettre.

   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, vous devez vérifier à nouveau votre identité lorsque vous enregistrez les modifications.

> **Vérification : l'héritage est actif**
>
> Si votre compte de gestion a activé l'héritage de vérification client, vous ne pouvez pas modifier ou soumettre vos propres informations de vérification client. Vos informations de vérification apparaissent en mode lecture seule.

1. Connectez-vous au Console de gestion AWS.
2. Dans la barre de navigation, dans le coin supérieur droit, choisissez le nom de votre compte (ou alias), puis cliquez sur 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 Soumettre.

   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.

Gérez l'héritage de vérification des clients pour AWS Organizations

Avec AWS Organizations, vous pouvez activer l'héritage des vérifications clients pour votre organisation. Lorsque vous activez l'héritage, les comptes India-based membres de votre organisation héritent du statut de vérification de votre compte de gestion. Ils n'ont pas besoin d'effectuer la vérification client de manière indépendante.

Votre compte de gestion doit effectuer sa propre vérification client avant de pouvoir activer l'héritage. Une fois que vous avez activé l'héritage, vous n'avez pas besoin de soumettre à nouveau vos documents de vérification.

Lorsque votre compte de gestion autorise l'héritage des vérifications clients, votre statut de vérification s'étend aux comptes des India-based membres de votre organisation. Pour ces comptes

de membres, nous pouvons utiliser ou divulguer vos informations de vérification en réponse à des demandes des forces de l'ordre ou réglementaires.

Activer ou désactiver l'héritage de vérification client

Suivez la procédure suivante pour activer ou désactiver l'héritage par validation client pour les comptes India-based membres de votre organisation.

1. Ouvrez le Console de gestion AWS chapeau Console de gestion AWS.
2. Dans la barre de navigation, choisissez le nom de votre compte (ou alias), puis sélectionnez Compte.
3. Sous Autres paramètres, sélectionnez Vérification du client.
4. Dans les paramètres de vérification du client, activez le bouton Héritage pour activer l'héritage ou désactivez-le pour le désactiver.
5. Passez en revue la boîte de dialogue de confirmation, puis confirmez votre choix.

Lorsque vous activez l'héritage, tous les comptes India-based membres de votre organisation héritent de votre statut de vérification. Lorsque vous désactivez l'héritage, nous rétablissons le statut de vérification antérieur pour les comptes membres qui ont déjà effectué leur propre vérification. Un compte de membre sans vérification préalable doit effectuer la vérification du client de manière indépendante.

Vérification du client pour AWS Comptes des membres des organisations

Si votre compte possède une adresse de India-based contact ou de facturation, vous héritez du statut de vérification du compte de gestion. Cela s'applique lorsque votre compte de gestion a activé l'héritage par vérification client. Vous pouvez voir un message sur la page de vérification du client qui le confirme.

Lorsque l'héritage est actif, vous ne pouvez pas soumettre ou modifier vos propres informations de vérification client. Vous n'avez aucune action à effectuer.

Si votre compte de gestion désactive l'héritage, vous devez disposer de votre propre statut de vérification client. Il en va de même si votre compte quitte l'organisation ou si le compte de gestion le supprime de l'organisation. Si vous avez déjà soumis vos propres informations de vérification, nous rétablissons votre statut de vérification antérieur. Il n'est pas nécessaire de répéter le processus. Cette restauration ne s'applique que si votre nom et votre adresse n'ont pas changé depuis votre dernière vérification.

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 suivants 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.
- Identification de l'électeur Card/EPIC - La carte d'identité de l'électeur, également connue sous le nom de carte d'identité avec photo des électeurs (EPIC), contient un numéro d'identification unique délivré par la Commission électorale de l'Inde aux électeurs éligibles en Inde. Un ID/EPIC numéro 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.
- 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' card/EPICélecteur et permis de conduire.
- 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, consultezthe section called "Configurez votre compte".

Utilisez le Console de gestion AWS 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 (TPS)
- Afficher une facture fiscale

Fermez un Compte AWS

Ces instructions indiquent comment fermer votre compte Compte AWS si vous vous êtes inscrit à AWS l'aide de l'option S'inscrire à AWS (version avancée) ou si vous avez activé les fonctionnalités avancées de votre compte. Pour comparer les options d'inscription, voirComparez les options d'inscription.

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 prendre en compte les points suivants :

- La fermeture de votre compte vous servira de notification de résiliation du contrat AWS client pour ce compte.
- Il n'est pas nécessaire de supprimer des ressources dans votre fichier Compte AWS avant de le fermer. Toutefois, nous vous recommandons de sauvegarder toutes les ressources ou données que vous souhaitez conserver. Pour obtenir des instructions sur la sauvegarde d'une ressource donnée, consultez la AWS documentation appropriée pour ce service.
- Vous pouvez rouvrir votre compte pendant la période suivant la fermeture. Les frais pour les services restés sur votre compte reprendront si vous le rouvrez. Vous restez également responsable de toutes les factures impayées, des instances réservées et des Savings Plans impayés.
- Vous demeurez responsable de tous les frais impayés et des charges relatifs aux services consommés avant la fermeture du compte. Vous recevrez une AWS facture le mois suivant la fermeture de votre compte. Par exemple, si vous avez fermé votre compte le 15 janvier, vous recevrez une facture début février pour l'utilisation effectuée entre le 1er et le 15 janvier. Vous continuerez à recevoir des factures pour les instances réservées et les Savings Plans après la fermeture de votre compte jusqu'à leur expiration.
- Vous ne pourrez plus accéder aux AWS services qui étaient auparavant disponibles dans votre compte. Cependant, vous pouvez vous connecter et accéder à un compte fermé Compte AWS pendant la période suivant la fermeture uniquement pour consulter les informations de facturation passées, accéder aux paramètres du compte ou contacter AWS Support.
- Vous ne pouvez pas utiliser 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 plus d'informations, consultez Mettez à jour le Adresse e-mail de l'utilisateur racine.
- Vous ne pouvez pas utiliser le même alias de compte que celui que vous avez enregistré Compte AWS au moment de sa fermeture pour un autre Compte AWS. Pour réutiliser l'alias pour un autre compte Compte AWS, supprimez-le avant de fermer le compte. Pour plus d'informations, consultez la section Utilisation d'un alias pour votre Compte AWS identifiant dans le guide de l'utilisateur IAM.
- 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 fermer que 20 % ou 250 des comptes de membres jusqu'à un maximum de 1 000 sur une période continue de 30 jours, selon le montant le plus élevé des deux. Ce quota n'est pas lié au mois civil, mais commence lorsque vous fermez un compte. 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.

Si l'adresse e-mail de l'utilisateur root de ce compte utilise un domaine enregistré via Route 53 dans ce même compte, ne fermez pas ce compte avant d'avoir effectué l'une des actions suivantes : transférer le domaine vers un autre Compte AWS ou mettre à jour l'adresse e-mail de l'utilisateur root pour utiliser un domaine qui n'est pas enregistré dans ce compte. Dans le cas contraire, la fermeture du compte suspend le domaine, ce qui interrompt la livraison des e-mails à votre adresse utilisateur root. Sans e-mail, vous ne pouvez pas récupérer le compte, et sans le compte, vous ne pouvez pas rétablir le domaine. Après 30 jours, Route 53 supprime définitivement le domaine. Cela s'applique également aux comptes membres dont les adresses e-mail de l'utilisateur root utilisent les domaines enregistrés dans ce compte.

- 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'une Compte AWS piste après la fermeture d'une piste, consultez Compte AWS la section Fermeture et pistes 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 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 Console de gestion AWS 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 rôle IAM.
2. Dans la barre de navigation en haut à droite, choisissez votre nom ou numéro de compte, puis Compte.

3. Sur la page Compte, choisissez le bouton Fermer le compte.
4. Entrez votre numéro 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. Choisissez le bouton Fermer le compte pour lancer le processus de clôture.
6. Vous devriez recevoir un e-mail confirmant la clôture de votre compte dans les minutes qui suivent.

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

Member account

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

Pour fermer un compte de membre depuis 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 Fermer le compte à côté du nom du compte en haut de la page. Cette option est disponible uniquement lorsqu'une organisation AWS est en mode Toutes les fonctionnalités.

> **Note**
>
> Si votre organisation utilise le mode de facturation consolidée, vous ne pourrez pas voir le bouton Fermer le compte dans la console. Pour fermer un compte en mode de facturation consolidée, connectez-vous au compte à fermer en tant qu'utilisateur racine. Sur la page Comptes, choisissez le bouton Fermer le compte, saisissez votre ID de compte, puis choisissez le bouton Fermer le compte.

4. Lisez les indications relatives à la clôture des comptes et assurez-vous de 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 membre que vous fermez affiche une étiquette `CLOSED` en regard de son nom dans la console AWS Organizations pendant une durée maximale de 90 jours à compter de la date de fermeture initiale. Après 90 jours, le compte du membre ne sera plus affiché dans la AWS Organizations console.

Pour clôturer un compte membre depuis la page Comptes

Vous pouvez éventuellement fermer un compte AWS membre directement depuis la page Compte du Console de gestion AWS. Pour obtenir des instructions étape par étape, suivez les instructions de l'onglet Compte autonome.

Cette option n'est pas disponible pour les comptes de projet qui n'ont pas d'utilisateur root. Fermez les comptes de projet depuis la AWS Organizations console.

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

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

Management account

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

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

Pour clôturer un compte de gestion depuis la page Comptes

1. Connectez-vous en Console de gestion AWS 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 rôle IAM.
2. Vérifiez qu'il ne reste aucun compte 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 `Closed` 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 en haut à droite, choisissez votre nom ou numéro de compte, puis Compte.
4. Sur la page Compte, choisissez le bouton Fermer le compte.
5. Entrez votre numéro 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. Choisissez le bouton Fermer le compte pour lancer le processus de clôture.
7. Vous devriez recevoir un e-mail confirmant la clôture de votre compte dans les minutes qui suivent.

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

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 fermeture.
- Tout compte de membre que vous fermez affichera une `CLOSED` 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.

Post-closure période

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, consultezRéouvrir un Compte AWS.

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

Réouvrir un Compte AWS

Si vous avez fermé votre compte Compte AWS et que vous n'avez pas de solde impayé, vous pouvez le rouvrir vous-même pendant la période suivant la fermeture.

Vous rouvrez votre compte en vous connectant en tant qu'utilisateur root et en soumettant la demande depuis la page Comptes.

Ce que vous devez savoir avant de rouvrir votre compte

Avant de rouvrir votre Compte AWS, prenez note des points suivants :

- Self-service exigences : Vous ne pouvez utiliser ce processus en libre-service que si vous avez fermé le compte vous-même et que votre compte n'avait aucun solde impayé au moment de la fermeture du compte. Vous devez vous connecter en tant qu'utilisateur root du compte fermé ; vous ne pouvez pas rouvrir un compte lorsque vous êtes connecté en tant qu'utilisateur ou en tant que rôle IAM. Vous devez soumettre votre demande de réouverture dans les 90 jours suivant la fermeture du compte, pendant la période suivant la fermeture.
- Comptes fermés par AWS : Si vous avez AWS fermé votre compte, vous ne pouvez pas le rouvrir vous-même. Payez tout solde impayé dans les 30 jours suivant la date de fermeture de votre compte, puis contactez-nous AWS Supportpour rouvrir votre compte.
- Paiements et frais : votre compte doit disposer d'un mode de paiement valide et non expiré. Comme votre facture du mois précédent est finalisée au début du mois suivant, il se peut que vous ayez un solde impayé pour utilisation avant la fermeture, même si votre compte n'avait aucun solde à la fermeture. Pour consulter ou payer un solde, consultez la section Effectuer des paiements. Lorsque vous rouvrez votre compte, les frais reprennent pour tous les services qui y sont toujours

en cours d'exécution. Si vous n'avez pas arrêté ces services avant de fermer le compte, vous avez peut-être également encouru des frais pendant la période suivant la fermeture.

Comment rouvrir votre compte

Suivez ces étapes pour rouvrir votre compte fermé.

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

Pour rouvrir votre compte depuis la page Comptes

1. Connectez-vous en Console de gestion AWS tant qu'utilisateur root du fichier fermé Compte AWS que vous souhaitez rouvrir. Vous ne pouvez pas rouvrir un compte lorsque vous êtes connecté en tant qu'utilisateur ou en tant que rôle IAM.
2. Ouvrez la page Comptes pour le compte fermé, comme suit : Dans la bannière du compte fermé, choisissez Rouvrir le compte.
3. Dans la boîte de dialogue Réouvrir le compte, entrez l'ID de compte affiché dans la boîte de dialogue pour confirmer que vous souhaitez rouvrir le compte.
4. Choisissez Rouvrir le compte pour soumettre votre demande. Un message confirme que la réouverture du compte a été initiée.
5. Attendez que la réouverture soit terminée. Lorsque votre compte est de nouveau actif, un message confirme que le compte a été rouvert avec succès et que vos AWS services et votre facturation ont été rétablis.

Si AWS vous ne parvenez pas à rouvrir votre compte, vous recevez une notification sur la console expliquant pourquoi et comment résoudre le problème.

À quoi s'attendre après la réouverture de votre compte

Une fois que vous avez soumis une demande de réouverture, voici ce qui se produit :

- Pour vérifier le statut, actualisez la page Comptes. Lorsque la réouverture est terminée, le compte apparaît comme actif et la bannière du compte fermé n'apparaît plus.
- Une fois le compte actif, AWS rétablit l'accès à ses services et ressources, et la facturation reprend.

Préparez votre compte en vue de son utilisation après sa réouverture

Certaines ressources et certains abonnements ne sont pas restaurés automatiquement. Après la réouverture de votre compte, vous devrez peut-être effectuer les opérations suivantes avant de pouvoir reprendre vos activités normales :

- Démarrez toutes les instances Amazon EC2 qui ont été arrêtées lors de la fermeture du compte. Pour plus d'informations, consultez Démarrer une instance dans le guide de l'utilisateur Amazon EC2.
- Restaurez les bases de données Amazon RDS à partir des instantanés créés lors de la fermeture du compte.
- Annulez et réabonnez-vous à tout AWS Marketplace abonnement. Les abonnements ne sont pas automatiquement restaurés lors de la réouverture du compte.

Disponibilité dans les Régions

Self-service la réouverture du compte est disponible dans toutes les régions commerciales.

Sécurité dans AWS Gestion du compte

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 organisations 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 responsable de la protection de l'infrastructure qui exécute AWS les services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Third-party les auditeurs testent et vérifient régulièrement l'efficacité de notre sécurité dans le AWS cadre des programmes de . Pour en savoir plus sur les programmes de conformité qui s'appliquent à la gestion des comptes, consultez Services AWS la section « portée par programme de conformité » ».
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Le modèle de responsabilité partagée est appliqué pour tous Comptes AWS. Cela inclut les comptes Comptes AWS que vous créez à l'aide de notre nouvelle AWS expérience et les comptes que vous créez à l'aide de notre AWS expérience avancée.

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 montre comment configurer la gestion des comptes pour atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également comment utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources de gestion de compte. Certains de ces documents ne concernent que les comptes créés grâce à notre AWS expérience avancée. Nous identifierons les cas où la documentation n'est pertinente que pour les comptes créés grâce à notre AWS expérience avancée.

Rubriques

- Protection des données dans AWS Gestion du compte
- AWS PrivateLink for AWS Gestion du compte
- Identity and Access Management pour AWS Gestion du compte

- AWS politiques gérées pour AWS Gestion du compte
- Validation de conformité pour AWS Gestion du compte
- Résilience dans AWS Gestion du compte
- Sécurité de l'infrastructure dans Gestion de compte AWS

Protection des données dans AWS Gestion du compte

Les informations suivantes sont pertinentes pour tous Comptes AWS.

Le modèle de responsabilité AWS https://aws.amazon.com/compliance/shared-responsibility-model/ s'applique à la protection des données dans la gestion des AWS comptes. Comme décrit dans ce modèle, AWS est responsable de la protection de l'infrastructure mondiale qui gère l'ensemble des 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 la FAQ sur la confidentialité des données et les conditions légales de la région . Pour plus d'informations sur la protection des données en Europe, consultez le Centre du règlement général sur la protection des données (RGPD).

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 Gestion des identités et des accès AWS (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.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation des activités des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour enregistrer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le Guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS cryptage, ainsi que tous les contrôles de sécurité par défaut qui s'y trouvent 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 à Services AWS l'aide de la console, de l'API ou des AWS kits de développement logiciel. 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 for AWS Gestion du compte

Les informations suivantes sont pertinentes pour tous Comptes AWS.

Si vous utilisez Amazon Virtual Private Cloud (Amazon VPC) pour héberger vos AWS ressources, vous pouvez accéder au service de gestion de AWS compte 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 sur les VPC, 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 Console de gestion AWS, du AWS Command Line Interface (AWS CLI), d'un AWS SDK, de l'API de gestion de AWS compte ou. 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 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 de CloudFormation, consultez la ressource AWS : :EC2 : :VPCENdpoint dans le Guide de l'utilisateur. CloudFormation

Politiques relatives aux terminaux Amazon VPC

Vous pouvez contrôler les actions qui peuvent être effectuées via ce point de terminaison de service en joignant 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 terminaux. Pour en savoir plus, consultez :

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

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

Les informations suivantes sont pertinentes pour tous Comptes AWS.

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 directeurs peuvent effectuer.
- La ressource sur laquelle les actions peuvent être effectuées.

L'exemple suivant illustre 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 secondaires de n'importe quel utilisateur Compte AWS, mais refuse à tous les utilisateurs IAM l'autorisation de supprimer toute autre information de contact sur n'importe quel compte.

Si vous souhaitez accorder l'accès à des comptes faisant partie d'une AWS organisation à un mandant qui se trouve dans 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 relatives aux terminaux, consultez la section Contrôle de l'accès aux services à l'aide de points de terminaison VPC dans le AWS PrivateLink Guide.

Identity and Access Management pour AWS Gestion du compte

Gestion des identités et des accès AWS (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources de gestion des comptes. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Les informations suivantes concernent Identity and Access Management pour la gestion des AWS comptes. Ces informations sont particulièrement pertinentes pour celles Comptes AWS que vous

créez lorsque vous utilisez notre AWS expérience avancée ou si vous avez activé des fonctionnalités avancées pour votre compte. Pour en savoir plus sur le fonctionnement du contrôle d'accès dans le cadre de notre nouvelle AWS expérience, consultezComparaison de la gestion des accès.

Rubriques

- Public ciblé
- Authentification par des identités
- Gestion de l'accès à l'aide de politiques
- Comment ? AWS La gestion des comptes fonctionne avec IAM
- Identity-based exemples de politiques pour AWS Gestion du compte
- Utilisation de politiques basées sur l'identité (politiques IAM) pour AWS Gestion du compte
- Résolution des problèmes AWS Identité et accès à la gestion des comptes

Public ciblé

La façon dont vous utilisez Gestion des identités et des accès AWS (IAM) varie en fonction de votre rôle :

- Utilisateur du service : demandez des autorisations à votre administrateur si vous ne pouvez pas accéder aux fonctionnalités (voir Résolution des problèmes AWS Identité et accès à la gestion des comptes)
- Administrateur du service : déterminez l'accès des utilisateurs et soumettez les demandes d'autorisation (voir Comment ? AWS La gestion des comptes fonctionne avec IAM)
- Administrateur IAM : rédigez des politiques pour gérer l'accès (voir Identity-based exemples de politiques pour AWS Gestion du compte)

Authentification par des identités

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

Vous pouvez vous connecter en tant qu'identité fédérée à l'aide d'informations d'identification provenant d'une source d'identité telle que AWS IAM Identity Center (IAM Identity Center), d'une authentification unique ou d'informations d'identification. Google/Facebook Pour plus d'informations

sur la connexion, consultez Connexion à votre Compte AWS dans le Guide de l'utilisateur Connexion à AWS .

Pour l'accès par programmation, AWS fournit un SDK et une CLI pour signer les demandes de manière cryptographique. Pour plus d'informations, consultez Signature AWS Version 4 pour les demandes d'API dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une seule identité de connexion appelée utilisateur Compte AWS root qui dispose d'un accès complet à toutes Services AWS les ressources. Il est vivement déconseillé d'utiliser l'utilisateur racine pour vos tâches quotidiennes. Pour les tâches qui requièrent des informations d'identification de l'utilisateur racine, consultez Tâches qui requièrent les informations d'identification de l'utilisateur racine dans le Guide de l'utilisateur IAM.

Identité fédérée

Il est recommandé d'obliger les utilisateurs humains à utiliser la fédération avec un fournisseur d'identité pour accéder à Services AWS l'aide d'informations d'identification temporaires.

Une identité fédérée est un utilisateur provenant de l'annuaire de votre entreprise, de votre fournisseur d'identité Web ou Directory Service qui y accède à Services AWS l'aide d'informations d'identification provenant d'une source d'identité. Les identités fédérées assument des rôles qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Pour plus d'informations, 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 qui dispose d'autorisations spécifiques pour une seule personne ou application. Nous vous recommandons d'utiliser ces informations d'identification temporaires au lieu des utilisateurs IAM avec des informations d'identification à long terme. Pour plus d'informations, voir Exiger des utilisateurs humains qu'ils utilisent la fédération avec un fournisseur d'identité pour accéder à AWS l'aide d'informations d'identification temporaires dans le guide de l'utilisateur IAM.

Les groupes IAM spécifient une collection d'utilisateurs IAM et permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. 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 dotée d'autorisations spécifiques qui fournit des informations d'identification temporaires. Vous pouvez assumer un rôle en passant d'un rôle utilisateur à un rôle IAM (console) ou en appelant une opération AWS CLI ou AWS API. Pour plus d'informations, consultez Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM sont utiles pour l'accès des utilisateurs fédérés, les autorisations temporaires des utilisateurs IAM, les accès intercompte, les accès entre services et les applications exécutées sur Amazon EC2. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Gestion de l'accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique définit les autorisations lorsqu'elles sont associées à une identité ou à une ressource. AWS évalue ces politiques lorsqu'un directeur fait une demande. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations les documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

À l'aide de politiques, les administrateurs précisent qui a accès à quoi en définissant 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. Un administrateur IAM crée des politiques IAM et les ajoute aux rôles, que les utilisateurs peuvent ensuite assumer. Les politiques IAM définissent les autorisations quelle que soit la méthode que vous utilisez pour exécuter l'opération.

Identity-based politiques

Identity-based les politiques sont des documents de politique d'autorisation JSON que vous attachez à une identité (utilisateur, groupe ou rôle). Ces politiques contrôlent les actions que peuvent exécuter ces identités, 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.

Identity-based les politiques peuvent être des politiques intégrées (intégrées directement dans une seule identité) ou des politiques gérées (politiques autonomes associées à plusieurs identités).

Pour découvrir comment choisir entre des politiques gérées et en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

Resource-based politiques

Resource-based les politiques sont des documents de politique JSON que vous attachez à une ressource. Les exemples incluent les politiques de confiance de rôle IAM et les stratégies de compartiment Amazon S3. 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. Vous devez spécifier un principal dans une politique basée sur les ressources.

Resource-based les politiques sont des politiques intégrées qui se trouvent dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Autres types de politique

AWS prend en charge des types de politiques supplémentaires qui peuvent définir les autorisations maximales accordées par les types de politiques les plus courants :

- Limites d'autorisations : une limite des autorisations définit le nombre maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM. Pour plus d'informations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCP) : spécifient les autorisations maximales pour une organisation ou une unité organisationnelle dans AWS Organizations. Pour plus d'informations, consultez Politiques de contrôle de service dans le Guide de l'utilisateur AWS Organizations .
- Politiques de contrôle des ressources (RCP) : définissent les autorisations maximales disponibles pour les ressources de votre organisation. Pour plus d'informations, consultez Politiques de contrôle des ressources (RCP) dans le Guide de l'utilisateur AWS Organizations .
- Politiques de session : politiques avancées que vous passez en tant que paramètre lorsque vous créez par programmation une session temporaire pour un rôle ou un utilisateur fédéré. 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 savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment ? AWS La gestion des comptes fonctionne avec IAM

Ces informations sont particulièrement pertinentes pour Comptes AWS celles que vous créez lorsque vous utilisez notre AWS expérience avancée. Pour en savoir plus sur le fonctionnement du contrôle d'accès dans le cadre de notre nouvelle AWS expérience, consultezComparaison de la gestion des accès.

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

Fonctionnalités IAM que vous pouvez utiliser avec AWS Gestion du compte

Fonctionnalité IAM	Assistance à la gestion des comptes
Identity-based politiques	Oui
Resource-based politiques	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique	Oui
ACL	Non
ABAC (étiquettes dans les politiques)	Non
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Rôles du service	Non
Service-linked rôles	Non

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

Identity-based politiques relatives à la gestion des comptes

Prend en charge les politiques basées sur l’identité : oui

Identity-based les politiques sont des documents de politique d'autorisation JSON que vous pouvez associer à une identité, telle qu'un utilisateur IAM, un groupe d'utilisateurs ou un rôle. 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. 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.

Identity-based exemples de politiques pour la gestion des comptes

Pour consulter des exemples de politiques de gestion des comptes basées sur l'identité, consultez. Identity-based exemples de politiques pour AWS Gestion du compte

Resource-based politiques relatives à la gestion des comptes

Prend en charge les politiques basées sur les ressources : non

Resource-based les politiques 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, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. 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 politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. 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 politique dans la gestion des comptes utilisent le préfixe suivant avant l'action.

```
account
```

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

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

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

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

Pour consulter des exemples de politiques de gestion des comptes basées sur l'identité, consultez. Identity-based exemples de politiques pour AWS Gestion du compte

Ressources relatives aux politiques pour la gestion des comptes

Prend en charge les ressources de politique : oui

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

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

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

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

- account

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

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

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

Pour consulter des exemples de politiques de gestion des comptes basées sur l'identité, consultez. Identity-based exemples de politiques pour AWS Gestion du compte

Clés de conditions de politique pour la gestion des comptes

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

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

L'élément `Condition` indique à quel moment les instructions s'exécutent en fonction de critères définis. 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. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

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

- compte : TargetRegion

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

- compte : AlternateContactTypes

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

  - FACTURATION
  - OPERATIONS
  - SECURITY

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

- compte : AccountResourceOrgPaths

  Cette clé de condition prend un argument qui consiste en une liste 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.

- compte : EmailTargetDomain

Cette clé de condition prend un argument qui consiste en une liste de domaines de messagerie. Il vous permet de filtrer la politique pour qu'elle n'affecte que les actions correspondant aux domaines de messagerie spécifiés. Cette clé de condition distingue les majuscules et minuscules. Vous devez utiliser `StringEqualsIgnoreCase` plutôt que `StringEquals` dans le bloc de conditions de la politique pour contrôler l'action en fonction du domaine d'adresse e-mail cible. Voici un exemple de politique permettant à l'`account:StartPrimaryEmailUpdate`action de s'exécuter lorsque le domaine de messagerie contient `example.comcompany.org`, ou une combinaison de cas, telle que`EXAMPLE.COM`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowConditionKey",
            "Effect": "Allow",
            "Action": [
                "account:StartPrimaryEmailUpdate"
            ],
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {
                    "account:EmailTargetDomain": [
                        "example.com",
                        "company.org"
                    ]
                }
            }
        }
    ]
}
```

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

Pour consulter des exemples de politiques de gestion des comptes basées sur l'identité, consultez. Identity-based exemples de politiques pour AWS Gestion du compte

Listes de contrôle d'accès dans la gestion des comptes

Prend en charge les ACL : non

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

Attribute-based contrôle d'accès avec gestion de compte

Prise en charge d’ABAC (balises dans les politiques) : non

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

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

Pour 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 pour les API de 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.

JSON

```
{
   "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 d'informations d'identification temporaires avec la gestion des comptes

Prend en charge les informations d'identification temporaires : oui

Les informations d'identification temporaires fournissent un accès à court terme aux AWS ressources et sont automatiquement créées lorsque vous utilisez la fédération ou que vous changez de rôle. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM et Services AWS compatibles avec IAM dans le Guide de l'utilisateur IAM.

Cross-service autorisations principales pour la gestion des comptes

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

Les sessions d'accès direct (FAS) utilisent les autorisations du principal appelant et Service AWS, combinées Service AWS à la demande d'envoi de demandes aux services en aval. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez la section Sessions de transmission 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.

Service-linked rôles 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 assumer le rôle d'effectuer une action en votre nom. Service-linked les rôles apparaissent dans votre fichier Compte AWS et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

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

Identity-based exemples de politiques pour AWS Gestion du compte

Ces informations sont particulièrement pertinentes pour Comptes AWS celles que vous créez lorsque vous utilisez notre AWS expérience avancée. Pour en savoir plus sur le fonctionnement du contrôle d'accès dans le cadre de notre nouvelle AWS expérience, consultezComparaison de la gestion des accès.

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources de gestion de compte. 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.

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 la gestion des comptes, y compris le format des ARN pour chacun des types de ressources, voir Actions, ressources et clés de condition pour la gestion des AWS comptes dans la référence d'autorisation de service.

Rubriques

- Bonnes pratiques en matière de politiques
- À l'aide de la page Compte du Console de gestion AWS
- Fournir un accès en lecture seule à la page Compte dans le Console de gestion AWS
- Fournir un accès complet à la page Compte dans le Console de gestion AWS

Bonnes pratiques en matière de politiques

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

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- 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 par le biais d'un service spécifique Service AWS, tel que 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.

- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger 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 Console de gestion AWS

Pour accéder à la page Compte dans le Console de gestion AWS, vous devez disposer d'un minimum d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter les détails de votre Compte AWS. Si vous créez une politique basée sur l'identité qui est plus restrictive que les autorisations minimales requises, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs et rôles IAM) tributaires de cette politique.

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

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

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

Dans l'exemple suivant, vous souhaitez accorder à un utilisateur IAM dans votre compte un accès en Compte AWS lecture seule à la page Compte du. Console de gestion AWS 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.

JSON

```
{
    "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 Console de gestion AWS

Dans l'exemple suivant, vous souhaitez accorder à un utilisateur IAM l'accès Compte AWS complet à la page Compte du Console de gestion AWS. 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.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "GrantFullAccessToAccountSettings",
```

```
            "Effect": "Allow",
            "Action": [
                "account:GetAccountInformation",
                "account:ListRegions",
                "account:PutContactInformation",
                "account:PutAlternateContact",
                "account:DeleteAlternateContact",
                "account:EnableRegion",
                "account:DisableRegion"
            ],
            "Resource": "*"
        }
    ]
}
```

Utilisation de politiques basées sur l'identité (politiques IAM) pour AWS Gestion du compte

Ces informations sont particulièrement pertinentes pour Comptes AWS celles que vous créez lorsque vous utilisez notre AWS expérience avancée. Pour en savoir plus sur le fonctionnement du contrôle d'accès dans le cadre de notre nouvelle AWS expérience, consultezComparaison de la gestion des accès.

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

Pour savoir comment mettre à jour les politiques gérées par le client, voir Modifier les politiques IAM dans le guide de l'utilisateur IAM.

AWS Politiques relatives aux actions de gestion des comptes

Ce tableau récapitule les autorisations qui permettent d'accéder aux paramètres de votre compte. Pour obtenir des exemples de stratégies qui utilisent ces autorisations, consultez Identity-based exemples de politiques pour AWS Gestion du compte.

> **Note**
>
> Pour accorder aux utilisateurs IAM un accès en écriture à un paramètre de compte spécifique sur la page Compte du Console de gestion AWS, 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`	List	Accorde l'autorisation de répertorier les régions disponibles.
`account:GetAccount Information`	Lecture	Accorde l'autorisation de récupérer les informations de compte d'un compte.
`account:GetAlterna teContact`	Lecture	Accorde l'autorisation de récupérer les contacts alternati fs d'un compte.
`account:GetContact Information`	Lecture	Accorde l'autorisation de récupérer les informations de contact principales d'un compte.
`account:GetPrimary Email`	Lecture	Accorde l'autorisation de récupérer l'adresse e-mail principale d'un compte.
`account:GetRegionO ptStatus`	Lecture	Accorde l'autorisation d'obtenir le statut d'opt-in d'une région.
`account:AcceptPrim aryEmailUpdate`	Écrire	Accorde l'autorisation d'accepter la mise à jour de l'adresse e-mail principale du compte membre d'une AWS organisation.
`account:CloseAccount`	Écrire	Accorde l'autorisation de fermer un compte.

Nom de l'autorisation	Niveau d'accès	Description
		Note Cette autorisation ne s'applique qu'à la console. Aucun accès API n'est disponible pour cette autorisation.
`account:DeleteAlternateContact`	Écrire	Accorde l'autorisation de supprimer les contacts alternatifs d'un compte.
`account:DisableRegion`	Écrire	Accorde l'autorisation de désactiver l'utilisation d'une région.
`account:EnableRegion`	Écrire	Accorde l'autorisation d'autoriser l'utilisation d'une région.
`account:PutAccountName`	Écrire	Accorde l'autorisation de mettre à jour le nom d'un compte.
`account:PutAlternateContact`	Écrire	Accorde l'autorisation de modifier les contacts alternatifs d'un compte.
`account:PutContactInformation`	Écrire	Accorde l'autorisation de mettre à jour les informations de contact principales d'un compte.

Nom de l'autorisation	Niveau d'accès	Description
`account:SendPhoneNumberVerification`	Écrire	Accorde l'autorisation d'envoyer un code de vérification au numéro de téléphone du contact principal d'un compte.
`account:StartPrimaryEmailUpdate`	Écrire	Accorde l'autorisation de lancer la mise à jour de l'adresse e-mail principale du compte membre d'une AWS organisation.
`account:VerifyPhoneNumber`	Écrire	Accorde l'autorisation de vérifier le numéro de téléphone du contact principal d'un compte en soumettant un code de vérification.

Résolution des problèmes AWS Identité et accès à la gestion des comptes

Ces informations sont particulièrement pertinentes pour Comptes AWS celles que vous créez lorsque vous utilisez notre AWS expérience avancée. Pour en savoir plus sur le fonctionnement du contrôle d'accès dans le cadre de notre nouvelle AWS expérience, consultezComparaison de la gestion des accès.

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

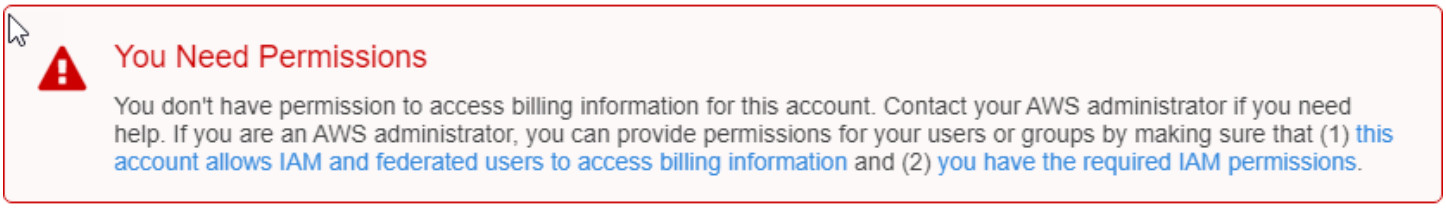
Rubriques

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

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

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

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



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

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

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

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

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

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

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

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

Je souhaite autoriser des personnes extérieures à mon Compte AWS pour accéder aux détails de mon compte

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

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir si la gestion des comptes prend en charge ces fonctionnalités, consultezComment ? AWS La gestion des comptes fonctionne avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour 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 AWS Gestion du compte

Ces informations sont particulièrement pertinentes pour celles Comptes AWS que vous créez lorsque vous utilisez notre AWS expérience avancée ou si vous avez activé des fonctionnalités avancées pour votre compte. Pour en savoir plus sur le fonctionnement du contrôle d'accès pour notre nouvelle AWS expérience, consultezComparaison de la gestion des accès.

AWS La gestion des comptes fournit actuellement deux politiques AWS gérées qui sont disponibles pour votre utilisation :

- AWS stratégie gérée : AWSAccountManagementReadOnlyAccess
- AWS stratégie gérée : AWSAccountManagementFullAccess
- Mises à jour de la gestion des comptes AWS stratégies gérées

Une politique AWS gérée est une politique autonome qui est 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 les autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont disponibles pour 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 que de nouvelles opérations d'API deviennent disponibles pour des services existants.

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

AWS stratégie gérée : AWSAccountManagementReadOnlyAccess

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 relatives à votre Comptes AWS
- Les Régions AWS qui sont activés ou désactivés pour Compte AWS (vous pouvez consulter l'état des régions dans votre compte uniquement à l'aide de la AWS console)

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

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `account`— Permet aux administrateurs de récupérer les informations de métadonnées relatives à Comptes AWS. Il permet également aux administrateurs de répertorier les éléments Régions AWS qui sont activés pour le compte dans le Console de gestion AWS.

JSON

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

AWS stratégie gérée : AWSAccountManagementFullAccess

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

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

- Les métadonnées relatives à votre Comptes AWS
- Les Régions AWS qui sont activés ou désactivés pour Compte AWS (vous pouvez consulter l'état 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 administrateurs de consulter ou de modifier les informations de métadonnées relatives à Comptes AWS. Il permet également aux administrateurs de répertorier les éléments Régions AWS qui sont activés pour le compte et de les activer ou de les désactiver dans le Console de gestion AWS.

JSON

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

Mises à jour de la gestion des comptes AWS stratégies gérées

Consultez les détails des mises à jour des 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 du compte.

Modifier	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 AWS Gestion du compte

Notre nouvelle AWS expérience ne peut être utilisée pour aucune charge de travail réglementée. Les informations suivantes concernent uniquement les comptes créés lorsque vous utilisez S'inscrire pour AWS (avancé).

Third-party les auditeurs évaluent la sécurité et la conformité des AWS services qui peuvent être exécutés sur votre site dans Compte AWS le cadre de multiples programmes de AWS conformité. Il s'agit notamment des certifications SOC, PCI, FedRAMP, HIPAA et d'autres.

Pour une liste des AWS services couverts par des programmes de conformité spécifiques, voir Services AWS Étendue par programme de conformité . Pour des informations générales, voir Programmes de AWS conformité Programmes .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, consultez la section Téléchargement de rapports dans la section AWS Artifact

Votre responsabilité en matière de conformité lors de l'utilisation de vos services Compte AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide en matière de sécurité et de conformité : ces guides de déploiement abordent les considérations architecturales et fournissent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture pour la sécurité et la conformité HIPAA sur Amazon Web Services — Ce livre blanc décrit comment les entreprises peuvent utiliser AWS cette technologie pour créer des applications. HIPAA-eligible

  > **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 — 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 de règles énoncées dans le guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure vos configurations de ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.

- AWS Security Hub CSPM— 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 AWS Gestion du compte

Les informations suivantes sont pertinentes pour tous Comptes AWS. Si vous utilisez notre nouvelle AWS expérience, des considérations régionales supplémentaires s'appliquent. Pour de plus amples informations, veuillez consulter Régions AWS pour vos projets.

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 Régions AWS les zones de disponibilité, consultez la section Infrastructure AWS globale.

Sécurité de l'infrastructure dans Gestion de compte AWS

Les informations suivantes sont pertinentes pour tous Comptes AWS.

En tant que services gérés, AWS les services qui s'exécutent sur votre réseau Compte AWS sont protégés par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et la manière de AWS protéger l'infrastructure, consultez AWS Cloud Security. 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 Security Pillar AWS Well-Architected Framework.

Vous utilisez les 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.
- Suites de chiffrement avec une confidentialité directe parfaite (PFS) telles que DHE (Ephemeral) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). 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

Cela inclut les comptes Comptes AWS que vous créez à l'aide de notre nouvelle AWS expérience et les comptes que vous créez à l'aide de notre AWS expérience avancée. Pour comparer les options d'inscription, consultezComparez les options d'inscription.

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 ou pour votre compte 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 qui ont appelé 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 Guide de l'utilisateur AWS CloudTrail.
- 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 de ressources. Les événements des AWS 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.

Logging AWS Appels d'API de gestion de compte utilisant AWS CloudTrail

Cela inclut les comptes Comptes AWS que vous créez à l'aide de notre nouvelle AWS expérience et les comptes que vous créez à l'aide de notre AWS expérience avancée. Pour comparer les options d'inscription, consultezComparez les options d'inscription.

Les API de gestion de AWS compte sont intégrées à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service qui appelle une opération de gestion de compte. CloudTrailcapture tous les appels d'API de gestion de compte sous forme d'événements. Les appels capturés incluent tous les appels destinés aux opérations de gestion

des comptes. Si vous créez un historique, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour les opérations de gestion des comptes. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents sur la CloudTrail console dans l'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, qui l'a faite et quand, ainsi que des informations supplémentaires.

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

Informations relatives à la gestion des comptes dans CloudTrail

CloudTrail est activée dans votre compte Compte AWS lorsque vous créez votre 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 permanent des événements qui vous concernent Compte AWS, y compris les événements liés aux opérations de gestion des comptes, créez un historique. Un journal permet CloudTrail de transmettre des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un parcours dans le Console de gestion AWS, le parcours s'applique à tous Régions AWS. Le journal d'activité consigne les événements de toutes les régions dans la partition AWS et livre les fichiers journaux dans le compartiment Simple Storage Service (Amazon S3) de votre choix. Vous pouvez configurer d'autres AWS services pour analyser plus en profondeur les données d'événements collectées dans les CloudTrail journaux et y donner suite. 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 répertoriées dans la section Référence des API de ce guide. Par exemple, les appels aux `PutAlternateContact`

opérations `CreateAccountDeleteAlternateContact`, 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 Gestion des identités et des accès AWS (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 journal 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 sont pas une pile 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 liés à la gestion des comptes avec EventBridge

Cela inclut les comptes Comptes AWS que vous créez à l'aide de notre nouvelle AWS expérience et les comptes que vous créez à l'aide de notre AWS expérience avancée. Pour comparer les options d'inscription, consultezComparez les options d'inscription.

Amazon EventBridge, anciennement appelé CloudWatch Events, vous permet de surveiller les événements spécifiques et de lancer des actions cibles qui en utilisent d'autres Services AWS. Les événements de Services AWS sont transmis 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 pour traitement.

Pour plus d'informations, consultez la section Premiers pas avec Amazon EventBridge dans le Guide de EventBridge l'utilisateur Amazon.

Événements liés 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 CloudTrail sont actuellement disponibles pour la gestion des comptes.

Types d'événements

- Événement pour l'activation et la désactivation des régions

Événement pour l'activation et la désactivation des régions

Lorsque vous activez ou désactivez une région dans un compte, 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 démarré, puis à nouveau une fois que l'un ou l'autre des processus sera terminé.

L'exemple d'événement suivant montre comment une demande sera envoyée en indiquant qu'il s'agissait `ENABLED` d'un compte `ap-east-1` dans `2020-09-30` la région`123456789012`.

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

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

- `ENABLED`— La région a été activée avec succès pour la zone `accountId` indiquée
- `ENABLING`— La Région est en train d'être activée pour `accountId` les
- `DISABLED`— La région a été désactivée avec succès pour la zone `accountId` indiquée
- `DISABLING`— La Région est en train d'être désactivée pour les personnes `accountId` indiquées

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

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

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

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

Quotas pour Gestion de compte AWS

Vous Compte AWS avez des quotas par défaut, anciennement appelés limites, pour chaque AWS service.

Les informations de quota suivantes concernent les projets que vous créez si vous utilisezInscrivez-vous pour AWS (nouveau). Pour ajuster un quota, créez un ticket d'assistance. Pour de plus amples informations, veuillez consulter Accompagnement de projets.

Ressource	Quota	Ajustable
Nombre de projets que vous possédez dans le cadre du plan gratuit	29	Non
Nombre de projets que vous pouvez acquérir dans le cadre du forfait payant	299	Non
Nombre de personnes avec lesquelles vous pouvez partager un projet	500	Non
Nombre d'invitations à des projets que vous pouvez accepter	100	Non

Les informations de quota suivantes Comptes AWS vous sont destinées à être créées si vous vous inscrivez à l'aide de l'option Inscription (avancée). Sauf indication contraire, chaque quota est Région AWS spécifique.

Ressource	Quota
Nombre maximum de `StartPrimaryEmailUpdate` demandes par compte cible	3 toutes les 30 secondes

Ressource	Quota
Nombre de contacts alternatifs dans un Compte AWS	3 - un pour chacun `BILLINGSECURITY`, et `OPERATIONS`
Nombre de demandes simultanées d'option de région par compte	6
Nombre de demandes simultanées d'option régionale par organisation	50
Taux de `AcceptPrimaryEmailUpdate` demandes par compte d'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 d'appelant	3 par seconde, rafale à 3 par seconde
Taux de `GetAlternateContact` demandes par compte	10 par seconde, rafale à 15 par seconde
Taux de `GetContactInformation` demandes par compte	10 par seconde, rafale à 15 par seconde
Taux de `GetGovCloudAccount Information` demandes par compte	3 par seconde, rafale à 5 par seconde
Taux de `GetPrimaryEmail` demandes par compte d'appelant	3 par seconde, rafale à 3 par seconde
Taux de `GetRegionOptStatus` demandes par compte	5 par seconde, rafale à 5 par seconde

Ressource	Quota
Taux de `ListRegions` demandes par compte	5 par seconde, rafale à 5 par seconde
Taux de `PutAccountName` demandes par compte d'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 d'appelant	1 par seconde, rafale à 1 par seconde

Historique des documents pour le guide de l'utilisateur de gestion de compte

Le tableau suivant décrit les versions de documentation relatives à la gestion des AWS comptes.

Modification	Description	Date
Nouvelles API de vérification des numéros de téléphone	Vous pouvez utiliser les nouvelles VerifyPhoneNumberAPI SendPhoneNumberVerificationet les API pour vérifier le numéro de téléphone du contact principal. La `GetContactInformation` réponse inclut également un nouveau `VerificationStatus` champ.	1 octobre 2026
Valeurs des quotas de fermeture de compte mises à jour	Le pourcentage de fermeture de comptes a été corrigé de 10 % à 20 % et le quota minimum de 10 à 250 dans la rubrique consacrée à la résolution des problèmes.	23 juin 2026
Nouvelles API de nom de compte	Support pour les nouveaux `GetAccountInformation` comptes et les `PutAccountName` API permettant d'afficher ou de modifier le nom d'un 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	6 janvier 2025

	du guide car le support est terminé.	
Nouvelles API de messagerie principales	Support pour les nouvelles `GetPrimaryEmail` `AcceptPrimaryEmail` `Update` API et pour mettre à jour de manière centralisée l'adresse e-mail de l'utilisateur root (adresse) 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	Gestion des identités et des accès AWS Les actions (IAM) précédemment utilisées pour gérer votre compte (par exemple, `aws-portal:ModifyAccount` et `aws-portal:ViewAccount`) ont atteint la fin du support standard.	1er janvier 2024
Réécriture du thème « Régions »	L'ensemble de la rubrique Régions a été complètement remanié, y compris l'ajout de commandes d'extension et de réduction.	8 octobre 2023
Rubriques relatives aux utilisateurs root déplacées vers le guide de l'utilisateur IAM	Discussion consolidée sur les utilisateurs root en une seule rubrique, ajout de liens de références croisées vers des sujets relatifs aux utilisateurs root qui ont été déplacés vers le guide de l'utilisateur IAM.	18 septembre 2023
Nouvelle section ajoutée à la rubrique de contact du compte principal	Ajout d'une nouvelle section sur les exigences relatives au numéro de téléphone et à l'adresse e-mail.	12 septembre 2023
Nouvelles API d'informations de contact	Support pour les nouveautés `GetContactInformation` et `PutContactInformation` les API.	22 juillet 2022

AWS La gestion des comptes prend désormais en charge la mise à jour des contacts alternatifs via la AWS Organizations console.	Vous pouvez désormais mettre à jour les contacts alternatifs de votre organisation via la AWS Organizations console à l'aide des autorisations de l'API de compte fournies par les politiques AWS Organizations gérées mises à jour.	8 février 2022
Première version	Publication initiale du guide de référence AWS sur la gestion des comptes	30 septembre 2021

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.