Guía del usuario de

AWS Administración de cuentas



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

AWS Administración de cuentas: Guía del usuario de

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

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

Qué es un Cuenta de AWS? 1
Características de un Cuenta de AWS 3
¿Es la primera vez AWS ¿usuario? 3
Soporte y comentarios 4
Otro AWS recursos 4
Compara las opciones de registro 6
compatible Servicios de AWS para Inscríbase en AWS (nuevo) 6
Servicios de AWS incluido en la capa gratuita de nuestra nueva AWS experiencia 7
Servicios de AWS incluido en el plan de pago de nuestro nuevo AWS experiencia 12
Servicios de AWS no es compatible con nuestro nuevo AWS experiencia 13
Consideraciones a la hora de elegir cómo registrarse AWS 18
Compare las funciones de las opciones de registro 19
Compare la gestión de acceso 20
Administre sus Cuentas de AWS 22
Registrarse en AWS (nuevo) 26
Inscríbase mediante Registrarse para AWS (nuevo) 28
Siguientes pasos 29
AWS Configuración de uso 30
Conecta una herramienta de codificación de IA 31
Consideraciones para conectar tu herramienta de codificación a tu proyecto 31
Conecta tu herramienta de codificación de IA a tu proyecto 32
Trabaja con varios proyectos 33
AWS acciones para los propietarios de proyectos 35
Actualiza tu contraseña 36
Gestionar la autenticación multifactor (MFA) 37
Puntos clave 37
Tipos de MFA disponibles para nuestro nuevo AWS experiencia 38
Registrar su dispositivo MFA de 40
Registrar una clave de seguridad como dispositivo MFA de 42
Cambie el nombre del dispositivo MFA de 42
Eliminar su dispositivo MFA 43
Eliminar todas las sesiones 43
Gestiona tu nombre o apodo 44
Cambia tu dirección de correo electrónico 45

Editar la información de contacto 46
Opte por no usar su contenido para mejorar el servicio 46
Solicita tus datos de AWS Builder ID 47
Crear un proyecto 48
Consideraciones para crear un proyecto 49
Para crear un proyecto 49
Regiones de AWS para tus proyectos 50
Busca la seleccionada Región de AWS para tus proyectos 51
Países en los que se aprovisionan recursos regionales en el este de EE. UU. (Ohio) (us-east-2) 51
Países en los que se aprovisionan recursos regionales en Asia Pacífico (Sídney) (ap-southeast-2) 54
Países en los que se aprovisionan recursos regionales en Europa (Estocolmo) (eu-north-1) 57
Políticas gestionadas para su organización 64
Políticas de control de servicios para proyectos 65
Políticas de control de servicios para la capa gratuita para proyectos 86
Políticas de control de servicios para el plan de pago para proyectos 97
Políticas de control de recursos para proyectos 109
Cambiar entre proyectos 111
Cambia de un proyecto a otro para ver las sesiones activas desde la Consola de administración de AWS 111
Cambia de un proyecto a otro en AWS Configuración 112
Cambia de un proyecto a otro desde el Consola de administración de AWS 112
Invita a los miembros del equipo 112
Consideraciones para los miembros del equipo 113
Cómo acceden los miembros del equipo a tu AWS recursos 114
Invita a los miembros del equipo 115
Invita a un miembro del equipo a un proyecto 115
Eliminar a un miembro del equipo de un proyecto 116
Eliminar a un miembro del equipo 117
Revocar una invitación 117
Reenviar una invitación 118
Actualiza tu cuenta 119
Consideraciones para actualizar tu cuenta 119
Actualiza tu cuenta 120

Creación de un límite de gasto 120
¿Qué es un límite de gasto? 120
Establece tu límite de gasto 121
Notificaciones 121
Personaliza la configuración de tus límites de gasto con controles de costes anticipados opcionales 122
¿Qué ocurre si alcanzas tu límite 123
Otros aspectos importantes que debes tener en cuenta 124
Crea un límite de gasto en AWS Configuración 124
Actualiza un límite de gasto 124
Actualiza un límite de gasto en AWS Configuración 125
Eliminar un límite de gasto 125
Eliminar un límite de gasto en AWS Configuración 126
Capa gratuita 126
Seguimiento del uso del nivel gratuito 127
Obtenga créditos adicionales 128
Consulta tu información de facturación en AWS Configuración 129
Para ver el costo por proyecto 129
Consulta tu historial de facturación en AWS Configuración 130
Gestiona tu método de pago 131
Realizar un pago en AWS Configuración 131
Cambia tu moneda preferida en AWS Configuración 132
Gestiona el registro de impuestos en AWS Configuración 133
Actualización y eliminación de números de identificación fiscal 133
Administrar sus exenciones fiscales de EE. UU. 133
Ver y canjear créditos 134
Administre las cuentas en India 135
Registrarse en AWS (nuevo) con AWS India 136
Administre la información de verificación del cliente 138
Configura tu facturación en India 141
Agregar o editar un número de cuenta permanente 142
Editar varios números de cuenta permanente 142
Editar varios números de impuestos de bienes y servicios 143
Ver una factura fiscal 143
Cambiar el nombre del vendedor registrado a o desde AWS India 143
Access AWS Support 145

Soporte para proyectos 146
Soporte técnico 147
Support si todos sus proyectos y organización están cerrados 147
Inicie una prueba de Business Support+ 147
Supervise su proyecto 148
Supervise su proyecto mediante AWS CloudTrail 148
Se usa CloudTrail para ver quién modificó el proyecto 149
Cerrar un proyecto 152
Lo que necesita saber antes de cerrar su proyecto 152
Para cerrar un proyecto 153
Post-closure periodo 153
Reabrir tu proyecto 154
Activa las funciones avanzadas 154
¿Qué ocurre cuando activas las funciones avanzadas 154
Proyecte las cuentas después de activar las funciones avanzadas 157
¿Cómo lo hará AWS ¿Cambiará la configuración después de activar las funciones avanzadas? 158
¿Puedo seguir creando un proyecto en AWS ¿Configuración después de activar las funciones avanzadas? 159
Cómo prepararse para activar las funciones avanzadas 159
¿Cómo activar las funciones avanzadas 160
Después de activar las funciones avanzadas 161
Establezca una contraseña de usuario root 161
Gestione los miembros de la fuerza 162
Cambiar la fuente de identidad 164
Eliminar las políticas de la organización 165
Cierra tu cuenta en AWS Configuración 167
Qué necesita saber antes de cerrar su cuenta de administración 168
Cerrar un proyecto 168
Cierre su cuenta de administración 168
Elimine su AWS ID de creador 169
Inscríbase en AWS (avanzado) 171
Paso 1: cree su cuenta 172
Paso 2: (recomendado) Instale el AWS CLI 174
Paso 3: (recomendado) Configurar el AWS Servidor MCP 175
Relacionado AWS servicios 175

Uso del usuario raíz ... 176
Acceso a su cuenta ... 177
Planificación de la estructura de gobernanza de su ... 178
Ventajas de usar múltiples Cuentas de AWS ... 179
Cuándo se debe usar AWS Organizations ... 181
Cuándo se debe usar AWS Control Tower ... 187
Descripción de los modos de operación de la API ... 188
Configure su cuenta ... 192
Creación o actualización del alias de cuenta ... 193
Activar o desactivar Regiones de AWS en tu cuenta ... 193
Actualiza la facturación de tu Cuenta de AWS ... 205
Actualizar el correo electrónico del usuario raíz ... 205
Actualizar la contraseña del usuario raíz ... 211
Actualiza tu Cuenta de AWS name ... 212
Actualiza los contactos alternativos de tu Cuenta de AWS ... 217
Actualiza el contacto principal de tu Cuenta de AWS ... 226
Vea los identificadores de su cuenta ... 237
Solución de problemas con su cuenta ... 243
Problemas de creación de cuentas ... 243
Problemas con el cierre de una cuenta ... 244
Otros problemas. ... 246
Administre las cuentas en India ... 247
Crea un Cuenta de AWS por AWS India ... 248
Administre la información de verificación del cliente ... 251
Cierre su cuenta ... 256
Qué debe saber antes de cerrar su cuenta ... 256
Cómo cerrar su cuenta ... 259
Qué esperar después de cerrar su cuenta ... 262
Vuelva a abrir su cuenta ... 263
Lo que debes saber antes de volver a abrir tu cuenta ... 264
¿Cómo volver a abrir tu cuenta ... 264
¿Qué puedes esperar después de volver a abrir tu cuenta ... 265
Prepara tu cuenta para usarla después de volver a abrirla ... 265
Disponibilidad por región ... 266
Protección de su cuenta ... 267
Protección de datos ... 268

AWS PrivateLink 269
Creación del punto de conexión 269
Políticas de punto de conexión de VPC de Amazon 270
Políticas de punto de conexión 270
Gestión de identidad y acceso 271
Público 272
Autenticación con identidades 272
Administración del acceso con políticas 273
AWS Administración de cuentas e IAM 275
Identity-based ejemplos de políticas 284
Uso de políticas basadas en identidades 288
Resolución de problemas 291
AWS políticas administradas 293
AWSAccountManagementReadOnlyAccess 294
AWSAccountManagementFullAccess 295
Actualizaciones de políticas 296
Validación de conformidad 296
Resiliencia 298
Seguridad de la infraestructura 298
Supervise su cuenta 300
CloudTrail registros 300
Información de administración de cuentas en CloudTrail 301
Descripción de las entradas de registros de Account Management 302
Supervisión de los eventos de administración de cuentas con EventBridge 305
Eventos de Account Management 306
Cuotas 309
Historial de revisión 312
..... cccxv

Qué es un Cuenta de AWS?

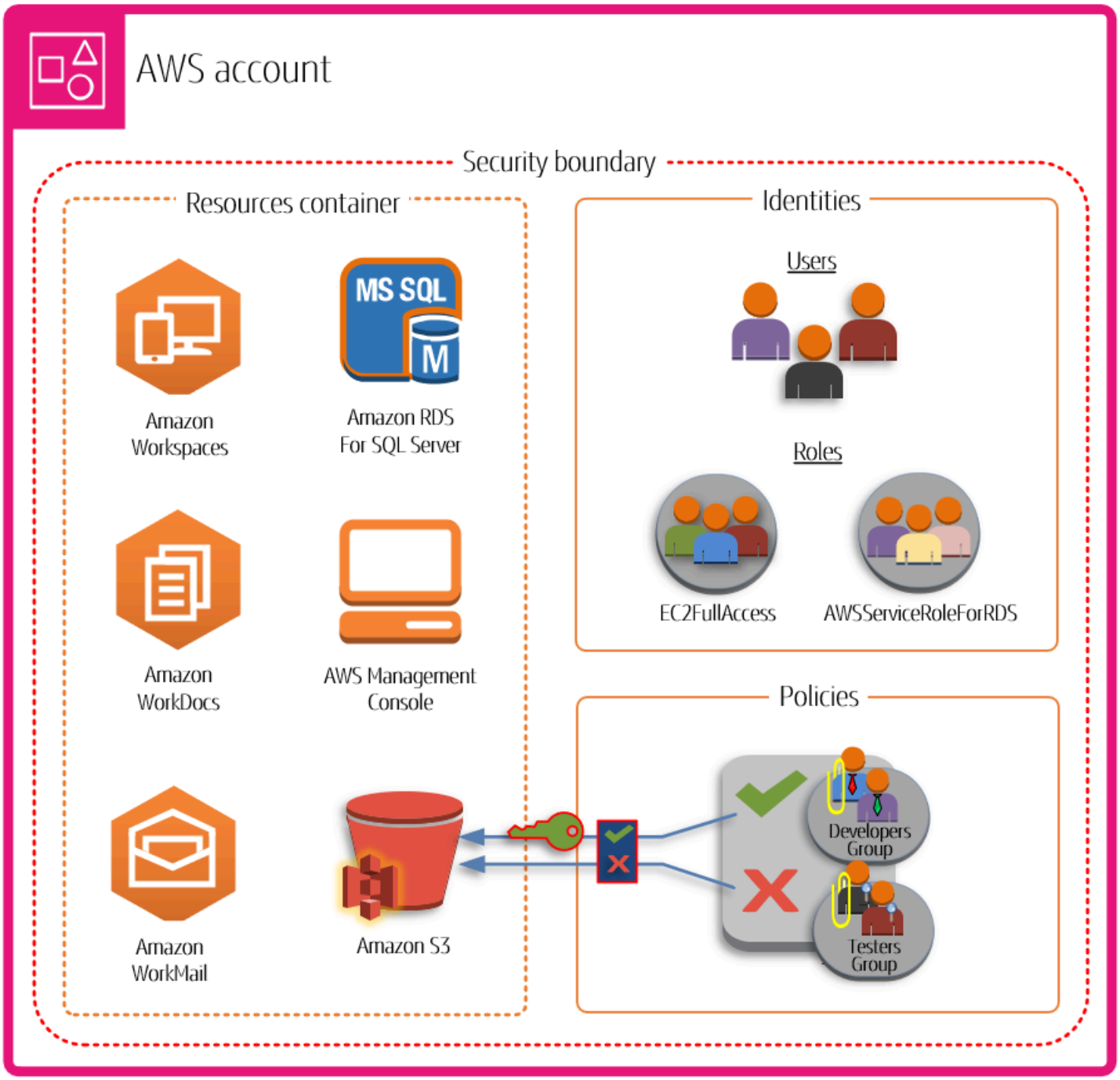
An Cuenta de AWS representa una relación comercial formal con la que usted establece AWS. Usted crea y administra sus AWS recursos en un Cuenta de AWS, y su cuenta proporciona capacidades de administración de identidades para el acceso y la facturación. Cada uno Cuenta de AWS tiene una identificación única que lo diferencia de los demás Cuentas de AWS.

Cuando te registras AWS, puedes elegir entre Registrarse AWS (nuevo) o Registrarse AWS (avanzado). En función de tu elección, puedes acceder a Cuentas de AWS nuestros proyectos. Los proyectos contienen Cuentas de AWS la configuración para compartirlos con otros colaboradores. Para obtener más información, consulte Compara las opciones de registro.

Sus recursos y datos en la nube están contenidos en una Cuenta de AWS. Una cuenta funciona como un límite de aislamiento de la administración de identidades y accesos. Cuando necesite compartir recursos y datos entre dos cuentas, deberá permitir este acceso de forma explícita. De forma predeterminada, no se permite el acceso entre cuentas. Por ejemplo, si designa cuentas diferentes para que contengan sus datos y recursos de producción y no producción, no se permitirá el acceso entre esos entornos de forma predeterminada.

Cuentas de AWS también son una parte fundamental del acceso a AWS los servicios. Como se muestra en la siguiente ilustración, un Cuenta de AWS cumple dos funciones principales:

- Contenedor de recursos: un Cuenta de AWS es el contenedor básico para todos los AWS recursos que creas como AWS cliente. Por ejemplo, un bucket de Amazon Simple Storage Service (Amazon S3), una base de datos de Amazon Relational Database Service (Amazon RDS) y una instancia de Amazon Elastic Compute Cloud (Amazon EC2) son todos recursos. Cada recurso se identifica de forma única mediante un nombre de recurso de Amazon (ARN) que incluye el ID de cuenta de la cuenta que contiene el recurso o que es propietaria del recurso.
- Límite de seguridad: An también Cuenta de AWS es el límite de seguridad básico de sus AWS recursos. Los recursos que crea en su cuenta están disponibles solo para los usuarios que tienen credenciales para su cuenta. Entre los recursos clave que puede crear en su cuenta se encuentran las identidades, como los usuarios y los roles. Las identidades tienen credenciales que alguien puede usar para iniciar sesión (autenticarse) en AWS. Las identidades también tienen políticas de permisos que especifican lo que un usuario puede hacer (autorización) con los recursos de la cuenta.



El uso de múltiples opciones Cuentas de AWS es una práctica recomendada para escalar su entorno, ya que proporciona un límite natural para la facturación de los costos, aísla los recursos para garantizar la seguridad, brinda flexibilidad a las personas y los equipos, además de adaptarse a los nuevos procesos empresariales. Para obtener más información, consulte Ventajas de usar múltiples Cuentas de AWS.

Características de un Cuenta de AWS

Cuentas de AWS incluyen las siguientes funciones principales:

- Supervise y controle los costos: una cuenta es el medio predeterminado para asignar AWS los costos. Por este motivo, usar diferentes cuentas para diferentes unidades de negocio y grupos de cargas de trabajo puede ayudarlo a rastrear, controlar, pronosticar, presupuestar e informar más fácilmente sus gastos en la nube. Además de los informes de costos a nivel de cuenta, AWS también cuenta con soporte integrado para consolidar e informar los costos de todo el conjunto de cuentas, en caso de que decida AWS Organizations utilizarlas en algún momento. También puede utilizar AWS Service Quotas para protegerse de un aprovisionamiento excesivo e inesperado de recursos de AWS y de acciones malintencionadas que podrían repercutir drásticamente en sus costos de AWS .
- Unidad de aislamiento: Cuenta de AWS proporciona límites de seguridad, acceso y facturación para tus AWS recursos, lo que puede ayudarte a lograr la autonomía y el aislamiento de los recursos. Por diseño, todos los recursos aprovisionados en una cuenta se aíslan lógicamente de los recursos aprovisionados en otras cuentas, incluso dentro de tu propio entorno. AWS Este límite de aislamiento le permite limitar los riesgos de que se produzcan problemas relacionados con la aplicación, una configuración incorrecta o acciones malintencionadas. Si hay un problema en una cuenta, los impactos en las cargas de trabajo de otras cuentas se pueden reducir o eliminar.
- Reflejo de las cargas de trabajo de su empresa: utilice varias cuentas para agrupar las cargas de trabajo con un objetivo empresarial común en cuentas distintas. Como resultado, puede alinear la propiedad y la toma de decisiones con esas cuentas y evitar dependencias y conflictos con la forma en que se protegen y administran las cargas de trabajo en otras cuentas. En función de su modelo empresarial general, puede optar por aislar distintas unidades de negocio o subsidiarias en cuentas diferentes. Este enfoque también podría facilitar la desinversión de esas unidades con el tiempo.

¿Es la primera vez AWS ¿usuario?

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Si es la primera vez que la utilizas AWS, el primer paso es registrarte. AWS Puedes crear un Cuenta de AWS sitio en el que tengas el control total de la configuración de la cuenta y donde se almacena tu contenido, algo que es necesario para las cargas de trabajo reguladas, como la HIPAA o el FedRAMP, o puedes crearlo con valores predeterminados preconfigurados. Cuentas de AWS Para saber qué registro es el más adecuado para usted, consulte. Compara las opciones de registro

Para obtener instrucciones paso a paso sobre cómo configurar una cuenta nueva en la que tengas el control total de la configuración inicial, consultaRegistrarse en AWS (avanzado).

Para obtener instrucciones paso a paso sobre cómo configurar una cuenta nueva que permita AWS crear cuentas con valores predeterminados preconfigurados, consulte. Registrarse en AWS (nuevo)

Compatibilidad con AWS Administración de cuentas

Puede publicar comentarios y hacer preguntas en el foro de soporte de AWS Account Management. Para obtener información general sobre AWS los foros, consulte AWS re:Post.

Si no encuentra las respuestas que busca en AWS re:Post, puede crear una cuenta o un caso de soporte relacionado con la facturación utilizando el Consola de administración de AWS. Para obtener más información, consulte Example: Create a support case for account and billing.

Otro AWS recursos

- AWS Capacitación y cursos: enlaces a cursos especializados y basados en roles, así como a laboratorios personalizados que le ayudarán a perfeccionar sus AWS habilidades y adquirir experiencia práctica.
- AWS Herramientas para desarrolladores: enlaces a herramientas y recursos para desarrolladores que proporcionan documentación, ejemplos de código, notas de la versión y otra información para ayudarle a crear aplicaciones innovadoras. AWS
- AWS Support Center: el centro para crear y administrar sus casos de AWS Support. También incluye enlaces a otros recursos útiles como foros, preguntas técnicas frecuentes, estado de los servicios y AWS Trusted Advisor.
- AWS Support: la página web principal con información sobre AWS Support, un canal de asistencia personalizada y de respuesta rápida que le ayuda a crear y ejecutar aplicaciones en la nube.
- Póngase en contacto con nosotros: un punto de contacto central para consultas relacionadas con la AWS facturación, la cuenta, los eventos, el uso indebido y otros problemas.

- AWS Condiciones del sitio: información detallada sobre nuestros derechos de autor y marca comercial; su cuenta, licencia y acceso al sitio; y otros temas.

Compara las opciones de registro

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Al registrarte AWS, accedes a la nube más completa y ampliamente adoptada del mundo. Ofrecemos la mejor selección de capacidades y experiencia innovadoras en la nube y la IA, en la infraestructura global más extensa, con seguridad, confiabilidad y rendimiento líderes del sector.

Hay dos formas de inscribirse AWS. Si desea tener un control total sobre la configuración de la cuenta y el lugar donde se almacena su contenido, o si tiene cargas de trabajo reguladas, como HIPAA o FedRAMP, úselo. Registrarse en AWS (avanzado) Si es un usuario nuevo y desea utilizar un nombre de usuario que ya tiene para iniciar sesión AWS y crear un AWS entorno con los valores predeterminados preconfigurados, seleccione, utilice. Regiones de AWSRegistrarse en AWS (nuevo)

compatible Servicios de AWS para Inscríbase en AWS (nuevo)

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Al usar la opción Registrarse para AWS (nueva), tendrás acceso a la capa gratuita. El nivel gratuito proporciona acceso a AWS servicios selectos. Puede actualizar su cuenta a un plan de pago para acceder a AWS servicios y funciones adicionales. Para obtener información sobre cómo actualizar tu cuenta, consultaActualiza tu cuenta en AWS Configuración.

No todos los AWS servicios están disponibles para registrarse AWS (nuevos). Si un servicio no aparece en ninguna de las siguientes listas o tiene una función no compatible, debe crear una cuenta utilizando Registrarse en AWS (avanzado) oActivar avanzado AWS Características de .

Servicios de AWS incluido en la capa gratuita de nuestra nueva AWS experiencia

Los siguientes AWS servicios están incluidos en la capa gratuita de Inscribirse AWS (nueva). Multi-Region o Las funciones entre regiones no son compatibles con ningún servicio. Para obtener más información, consulte Regiones de AWS para tus proyectos.

- Amazon API Gateway
- Amazon Athena
- Amazon AppFlow
- AWS App2Container
- Amazon Augmented AI
- Amazon Bedrock
- Amazon Bedrock Agent Core
- Amazon CloudFront
  - Lambda @Edge no es compatible.
- Amazon CloudWatch
- Amazon CloudWatch Logs
- Amazon CodeGuru Profiler
- Amazon Cognito
- Amazon Cognito Sync
- Amazon DynamoDB
- Amazon DataZone
- Amazon Elastic Container Registry (ECR)
- Generador de Imágenes de EC2
- Amazon EKS Anywhere
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
  - No se admiten el bloque de capacidad de compra ni la extensión del bloque de capacidad de compra.
- 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
- Servicio administrado por Amazon para Prometheus
- Amazon Managed Workflows para Apache Airflow
- Amazon MQ
- OpenSearch Servicio Amazon
- Amazon Polly
- Amazon Quick
  - Solo se admiten Amazon Quick Free o Quick Plus. Para obtener más información, consulta los precios rápidos de Amazon.
- 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
  - No se admiten Amazon S3 Access Grants.
- Amazon Simple Workflow Service
- Amazon Verified Permissions

- Amazon Virtual Private Cloud
- Amazon Aurora
- Amazon Aurora DSQL
- AWS Amplify
- AWS AppConfig
- AWS AppSync
- Aplicación de escalado automático
- AWS Transform MGN
- AWS Artifact
  - No se admiten el Apéndice de Asociado Comercial (HIPAA), el Apéndice de Asociado AWS Empresarial (HIPAA) AWS Organizations, el Apéndice de la Regla 17a-4 de la AWS SEC y el Apéndice de la Regla 18a-6 de la SEC. AWS
- Intercambio de datos de AWS B2B
- Agente de AWS Backint
- AWS Backup
- AWS Batch
- Administración de facturación y costos de AWS
  - Usa los AWS ajustes para configurar tu facturación, crear límites de gastos para controlar tus costos y recuperar y pagar las facturas. Utiliza Billing and Cost Management para crear presupuestos, analizar y optimizar sus costos. Para obtener más información, consulte Uso de la consola Billing and Cost Management con nuestra nueva AWS experiencia.
- AWS Budgets
- AWS Gestor de certificados
  - AWS No se admiten los certificados públicos exportables de Certificate Manager.
- API de control de nube de AWS
- AWS Cloud Map
- AWS Cloud9
- AWS CloudFormation
- AWS CloudShell
- AWS CloudTrail

- AWS CodeArtifact
- AWS CodeCommit
- AWS CodeDeploy
- AWS CodePipeline
- AWS Compute Optimizer
- AWS Config
- AWS Console Mobile Application
- AWS Cost Explorer
- AWS Data Pipeline
- AWS Transferencia de datos
- AWS DataSync
- AWS Directory Service
- AWS Elastic Beanstalk
- AWS End User Messaging Social
- AWS Entity Resolution
- AWS Glue
- AWS Health
- AWS Identity and Access Management
- AWS IoT
  - AWS Greengrass no es compatible.
- AWS IoT Device Defender
- AWS IoT Administración de dispositivos
- AWS IoT SiteWise
- AWS IoT TwinMaker
- AWS Key Management Service
- AWS Lake Formation
- AWS Lambda
  - Lambda @Edge no es compatible.
- AWS Launch Wizard

- AWS License Manager
- Consola de administración de AWS
- AWS Marketplace
  - Solo Bedrock y Free.
- AWS Network Manager
- AWS Payment Cryptography
- AWS PrivateLink
- AWS Resource Access Manager (RAM)
- Explorador de recursos de AWS
- Grupos de recursos de AWS
- Controlador de recuperación de aplicaciones (ARC) de Amazon Route 53
- AWS SDK y herramientas
- AWS Secrets Manager
- AWS Security Token Service
- AWS Serverless Application Repository
- Service Quotas
- AWS Signer
- AWS Step Functions
- AWS Support
- AWS Systems Manager
- AWS Systems Manager para SAP
- AWS User Notifications
  - User-configured no se admiten las notificaciones ni las operaciones de configuración de notificaciones administradas. Para obtener más información, consulte ¿Qué son las notificaciones AWS de usuario?
- AWS WAF
  - AWS Shield no es compatible.
- AWS Well-Architected Tool
- AWS X-Ray
- AWS CodeBuild

- Elastic Load Balancing
- AWS SQL Workbench
- Amazon OpenSearch Service sin servidor
- Amazon Timestream

Para ver la política que controla el acceso a los servicios de la capa gratuita, consulte Políticas de control de servicios para la capa gratuita para proyectos.

Servicios de AWS incluido en el plan de pago de nuestro nuevo AWS experiencia

Los siguientes servicios están disponibles para registrarse AWS (nuevos) si tiene un plan de pago. Para obtener más información, consulte Actualiza tu cuenta en AWS Configuración. Multi-Region o Las funciones entre regiones no son compatibles con ningún servicio. Para obtener más información, consulte Regiones de AWS para tus proyectos.

- El DevOps gurú de Amazon
- Amazon DocumentDB (compatible con MongoDB)
- Amazon EMR
- Amazon Forecast
- Amazon Glacier
- Amazon Kinesis
- Amazon Kinesis Data Streams
- Amazon Data Firehose
- Amazon Kinesis Video Streams
- Amazon Managed Blockchain
- Transmisión administrada de Amazon para 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 Agente de seguridad
- AWS Storage Gateway
- DevOps Agente

Para ver la política que controla el acceso a los servicios del plan de pago, consultePolíticas de control de servicios para el plan de pago para proyectos.

Servicios de AWS no es compatible con nuestro nuevo AWS experiencia

Los siguientes AWS servicios no son compatibles con nuestra nueva AWS experiencia, a menos que ustedActivar avanzado AWS Características de . Estos AWS servicios no son necesarios para los nuevos desarrolladores o los equipos pequeños. Algunos de estos servicios se activan automáticamente en tu cuenta y son gestionados por AWS. Para obtener más información, consulte Compare las funciones de las opciones de registro.

- Alexa for Business
- Alexa Top Sites
- Alexa Web Information Service
- Amazon Braket
- Amazon Chime
- Amazon Chime Business Calling, un servicio vendido por AMCS LLC
- Amazon Chime Llámame
- Amazon Chime Call Me, un servicio vendido por AMCS LLC

- Amazon Chime Dial In, un servicio vendido por AMCS LLC
- Amazon Chime Dialin
- Características de Amazon Chime
- Amazon Chime SDK
- Servicios Amazon Chime
- SMS DE Amazon Chime
- Amazon Chime Voice Connector, un servicio vendido por AMCS LLC
- Amazon Cloud Directory
- Amazon CloudSearch
- Amazon CodeWhisperer
- Amazon Connect Customer
- Perfiles de clientes de Amazon Connect Customer
- Amazon Connect Customer Voice ID
- AWS Deadline Cloud
- Amazon Detective
- Amazon Elastic Inference
- Amazon Elastic Transcoder
- Amazon FinSpace
- Flota flexible de Amazon
- Amazon Fraud Detector
- Amazon FSx
- GameLift Servidores Amazon
- Amazon GameLift Streams
- Amazon GameSparks
- Amazon GuardDuty
- AWS HealthOmics
- Amazon Inspector Classic
- Amazon Interactive Video Service
- Chat de Amazon IVS

- Amazon Kendra
- Amazon Keyspaces (para Apache Cassandra)
- Kiro
- Amazon Macie
- Amazon Managed Grafana
- Amazon Mechanical Turk
- Recompensas a los trabajadores de Amazon Mechanical Turk
- Amazon Mobile Analytics
- Amazon Monitron
- Amazon Nimble Studio
- OpenSearch Servicio de ingestión de Amazon Service
- Amazon Q
- Amazon Q Business
- Amazon Q Developer
- Amazon Quantum Ledger Database (Amazon QLDB)
- Amazon S3 en Outposts
- Amazon SageMaker Ground Truth
- Amazon Security Lake
- Amazon Sumerian
- Amazon WorkDocs
- Amazon WorkSpaces
- WorkSpaces Instancias de Amazon
- WorkSpaces Aplicaciones Amazon (Amazon WorkSpaces Applications)
- Amazon WorkSpaces Thin Client
- Amazon WorkSpaces Web
- Amazon WorkLink
- Amazon WorkMail
- AWS Elaborador de perfiles de costes de aplicaciones
- AWS Clean Rooms

- AWS Estudio de aplicaciones
- AWS Application Discovery Service
- AWS Audit Manager
- AWS Billing Conductor
- AWS CloudHSM
- AWS Client VPN
- AWS WAN en la nube
- AWS Control Tower
- AWS Database Migration Service
- AWS DeepRacer
- AWS Device Farm
- AWS Direct Connect
- AWS Elastic Disaster Recovery
- 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 Interconexión
- AWS IoT Eventos
- 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
- Calculadora de precios de AWS
- AWS Autoridad de certificación privada
- AWS Proton
- AWS re:Post Private
- AWS Resilience Hub
- AWS RoboMaker
- AWS Tejido RTB
- AWS Security Hub
- AWS Security Incident Response
- AWS Service Catalog
- AWS Shield
- AWS SimSpace Weaver
- AWS Snowball
- AWS Supply Chain
- Creador de redes de telecomunicaciones de AWS
- AWS Transform
- AWS Transfer Family
- AWS Transit Gateway
- AWS Trusted Advisor
- Acceso verificado de AWS

- Site-to-Site VPN
- Amazon VPC Lattice
- AWS Wickr
- Amazon CodeCatalyst
- Amazon Comprehend Medical
- Telecomunicaciones para conferencias (servicio vendido por AMCS LLC)
- Contact Center Telecommunications (servicio vendido por AMCS LLC)
- Contact Center Telecommunications Korea
- Contact Center Telecommunications Sudáfrica
- DynamoDB Accelerator
- Amazon Elastic VMware Service
- Oracle Database@AWS
- Red Hat OpenShift Service en AWS
- AWS App Runner

Consideraciones a la hora de elegir cómo registrarse AWS

Ten en cuenta lo siguiente antes de elegir tu método de registro. Si es necesario, puedes activar todas AWS las funciones de tu cuenta.

- Si tiene requisitos de producto específicos, como cargas de trabajo reguladas que incluyen HIPAA o FedRAMP, no utilice nuestra nueva experiencia. AWS
- Su contenido se almacenará en una región designada, que se seleccionará en función de su información de contacto.
- La nueva AWS experiencia te facilita empezar a crear sin necesidad de crear AWS permisos. Si necesita un control detallado sobre sus usuarios o permisos basados en funciones, no utilice Sign up for (nuevo). AWS
- Si necesitas configurar los pagos específicos de cada cuenta mediante AWS, lo que también se conoce como facturación en condiciones netas, no utilices Sign up for (nuevo). AWS
- Si necesitas acceder al conjunto completo de AWS servicios, no utilices Registrarse para AWS (nuevo). Para obtener más información, consulte compatible Servicios de AWS para Inscríbase en AWS (nuevo).

Compare las funciones de las opciones de registro

En la siguiente tabla, AWS se comparan los requisitos generales que se admiten para la AWS suscripción (nueva) o para la suscripción AWS (avanzada). Si una función no aparece en esta tabla o no se describe en ellaCompare la gestión de acceso, está disponible. Puedes activar las funciones avanzadas de tu cuenta si necesitas alguna de las funciones no compatibles. Para obtener más información, consulte Activar avanzado AWS Características de .

Característica	Inscríbase en AWS (nueva)	Inscríbase en AWS (avanzado)
Únase a AWS Partner Network	No	Sí
Cree un contrato de servicios profesionales	No	Sí
Inscríbase en un acuerdo empresarial con AWS	No	Sí
Adquiera una suscripción a AWS Skill Builder Team	No	Sí
Trabaja con un compañero AWS de formación	No	Sí
Obtenga créditos adicionales con AWS Activate	No	Sí
Usa AWS Marketplace	No	Sí
Designa tu AWS cuenta como compatible con la HIPAA o la SEC	No	Sí
Seleccione uno específico Región de AWS para crear sus recursos regionales	No. Para obtener más información, consulteRegiones de AWS para tus proyectos.	Sí
Acceda a una región de suscripción voluntaria	No	Sí
IAM Access Analyzer	No	Sí

Característica	Inscríbase en AWS (nueva)	Inscríbase en AWS (avanzado)
Sign-in políticas de acceso	No	Sí
Crea límites de gasto para tus cuentas	Sí	No
Savings Plans	No	Sí
Suscripción automática al Centro de optimización de costos para el plan de pago	Sí	No
Suscripción automática a AWS Organizations	Sí	No
Inscripción automática al IAM Identity Center	Sí	No
Inscríbase automáticamente en el administrador de funciones de IAM	Sí	No
Colores de las cuentas de consola	No	Sí
Utilizar AWS Console Mobile Application	No	Sí
Inhabilite la compatibilidad con consolas multisesión	No	Sí. Si vuelves a iniciar sesión con un Builder ID, la compatibilidad multisesión se habilitará automáticamente.

Compare la gestión de acceso

Cuando utilizas nuestra nueva AWS experiencia, AWS crea valores predeterminados preconfigurados para ayudarte a empezar a crear. Sus AWS recursos están organizados en proyectos. Un proyecto contiene una Cuenta de AWScuenta de proyecto y una configuración para compartirla con otros colaboradores. Si utilizas el plan de pago, tu proyecto también puede tener un coste mensual fijo antes de impuestos, denominado límite de gasto. Todos los proyectos de tu propiedad forman parte de tu organización, que puedes controlar a través de tu cuenta de

administración en AWS Configuración. Esta organización es lo mismo que una AWS organización; sin embargo, AWS gestiona aspectos de esta organización en tu nombre.

AWS administra los siguientes elementos de su AWS organización:

- Políticas de gestión de la organización. Al utilizar nuestra nueva AWS experiencia, AWS gestiona las políticas de gestión de la organización, incluidas las políticas de control de recursos (RCP) y las políticas de control de servicios (SCP). Si quieres crear las tuyas propias, usa Sign up for AWS (avanzado).
- Funciones de acceso humano. Un rol de acceso humano es cualquier rol que otorga permisos específicos a un humano. AWS te proporciona a ti y a los miembros de tu equipo acceso de administrador a tus proyectos. Como propietario del proyecto, puedes añadir y eliminar miembros del equipo. Para obtener más información, consulte Invita a los miembros del equipo a colaborar en AWS Configuración. No se crea un usuario root. Tu AWS Builder ID es el propietario de tus cuentas de proyecto y no de la dirección de correo electrónico del usuario raíz, y esto no cambia cuando activas las funciones avanzadas. Puedes crear roles de IAM y usuarios de IAM si es necesario, pero solo se pueden usar para el acceso mediante programación, no para el acceso a la consola.

Cada proyecto tiene una implementación de seguridad gestionada que facilita la creación con confianza. De forma predeterminada, cualquier aplicación o código del proyecto tiene acceso a todos AWS los recursos del mismo proyecto. No es necesario realizar una configuración de acceso adicional.

AWS los recursos de distintos proyectos no pueden acceder entre sí, a menos que actives el acceso entre proyectos para determinados recursos. Por ejemplo, puede crear una función Lambda en un proyecto y, a continuación, invocarla mediante una API en otro proyecto. Esto se describe como una integración entre cuentas. Para obtener más información, consulte Integraciones de Cross-accountLambda. Siempre y cuando ambos proyectos pertenezcan a la misma cuenta de administración, se admite.

De forma predeterminada, el proyecto no proporciona acceso externo a ningún recurso. Debe configurar AWS los recursos para permitir el acceso público. Se puede hacer lo siguiente:

- Cree un bucket de S3 público para alojar un sitio web o archivos estáticos simples. Para obtener más información, consulte Introducción a Amazon S3.
- Cree una API API Gateway que sirva de puerta de entrada a su aplicación. Para obtener más información, consulta Cómo crear una API HTTP.

- Cree una instancia EC2 con una dirección IP pública para permitir la comunicación entre sus instancias e Internet. Para obtener más información, consulte Lance su primera instancia EC2.
- Cree una CloudFront distribución para entregar su contenido web estático y dinámico, como .html, .css, .js y archivos de imagen, a sus usuarios. Para obtener más información, consulte Primeros pasos con. CloudFront
- Cree una URL de función de Lambda para proporcionar un punto de enlace HTTP simple y directo de acceso público para una función de Lambda. Asegúrese de que la función Lambda tiene los permisos correctos. Para obtener más información, consulte Creación de una URL de función y Modelo de seguridad y autenticación para las URL de funciones de Lambda.
- Utilice una combinación de estos u otros mecanismos. AWS

Además, al activar las funciones avanzadas, tiene acceso a aún más mecanismos para proporcionar acceso externo a sus recursos.

Administre sus Cuentas de AWS

Usted administra sus Cuentas de AWS datos en función del tipo AWS que utilice. En la siguiente tabla se muestra dónde encontrar la documentación de cada tarea de administración.

Tarea	Registrarse en AWS (nuevo)	Registrarse en AWS (avanzado)
Inscríbase	Registrarse en AWS (nuevo)	Registrarse en AWS (avanzado)
Creación de una cuenta de	Crea un proyecto en AWS Configuración	Registrarse en AWS (avanzado)
Cierre de una cuenta	Cerrar un proyecto en AWS Configuración	Cerrar un Cuenta de AWS
Actualiza tu contraseña	Actualiza tu contraseña en AWS Configuración	Actualizar la contraseña del usuario raíz

Tarea	Registrarse en AWS (nuevo)	Registrarse en AWS (avanzado)
Registrar dispositivos MFA	Gestione la autenticación multifactor (MFA) en AWS Configuración	Paso 3: (recomendado) Configurar el AWS Servidor MCP
Cambia tu correo electrónico	Cambia tu dirección de correo electrónico en AWS Configuración	Actualiza el dirección de correo electrónico del usuario raíz
Cambia tu nombre	Gestiona tu nombre o apodo en AWS Configuración	Actualiza tu Cuenta de AWS name
Actualiza la información de contacto	Edita tu información de contacto en AWS Configuración	Actualiza el contacto principal de tu Cuenta de AWS
Actualizar contactos alternativos	No aplicable	Actualiza los contactos alternativos de tu Cuenta de AWS
Administra la facturación	Gestiona tu método de pago en AWS Configuración	Actualiza la facturación de tu Cuenta de AWS
Administra la información tributaria	Gestiona el registro de impuestos en AWS Configuración	Administre sus pagos
Activar o desactivar Regiones de AWS	No se usa. No puede modificar su Región de AWS.	Activar o desactivar Regiones de AWS en tu cuenta

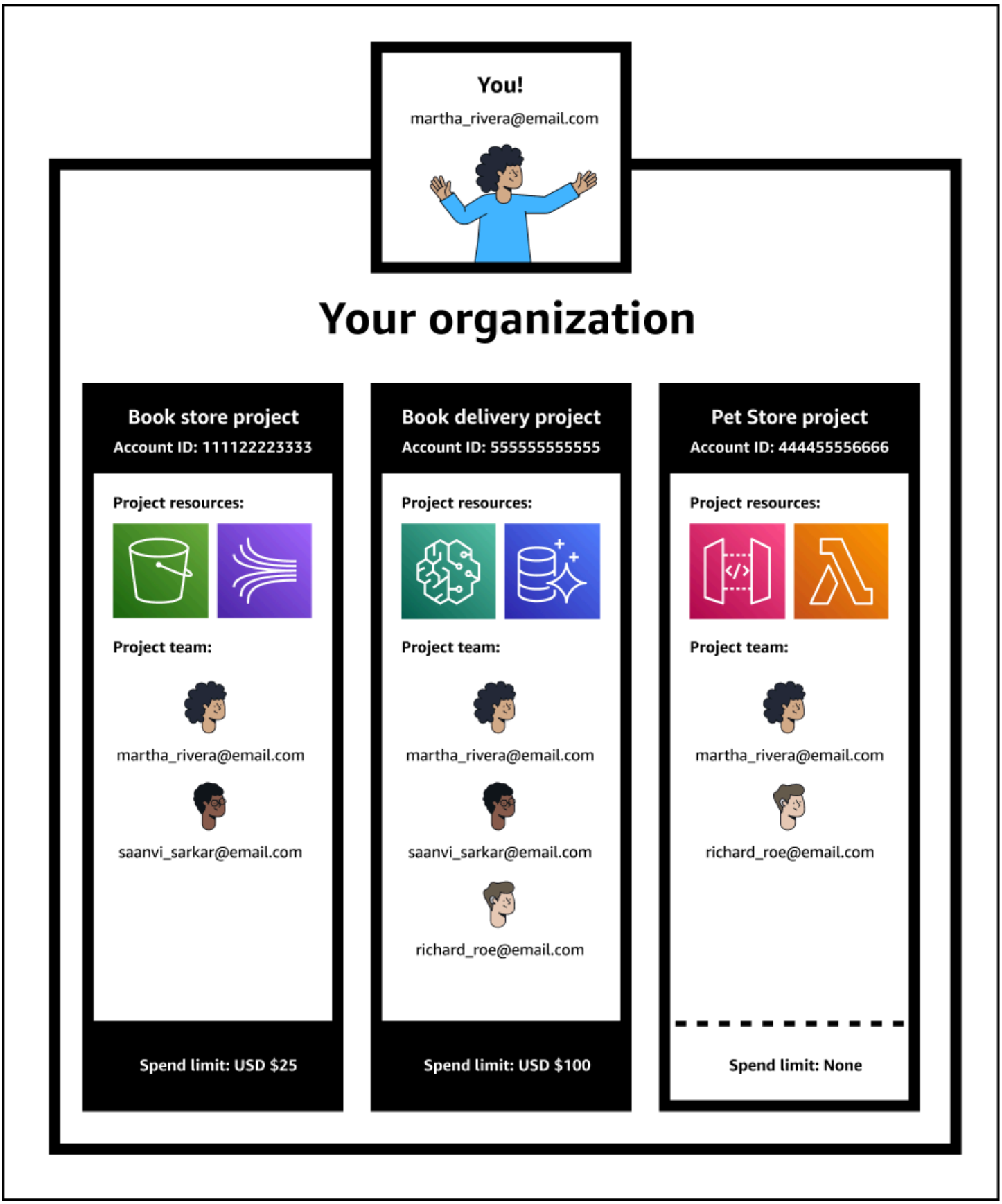
Tarea	Registrarse en AWS (nuevo)	Registrarse en AWS (avanzado)
Ver los identificadores de la cuenta	No aplicable	Visualización Cuenta de AWS identific adores
Crear un alias de cuenta	No aplicable	Crea un Cuenta de AWS alias
Actualice su cuenta	Actualiza tu cuenta en AWS Configuración	Planes de nivel gratuitos
Creación de un límite de gasto	Crea un límite de gasto en AWS Configuración	No aplicable
Actualiza un límite de gasto	Actualiza un límite de gasto en AWS Configuración	No aplicable
Eliminar un límite de gasto	Eliminar un límite de gasto en AWS Configuración	No aplicable
Invita a los miembros del equipo	Invita a los miembros del equipo a colaborar en AWS Configura ción	Identidades de IAM
Cambie de un proyecto a otro	Cambiar entre proyectos	Multi-session apoyo
Conecta una herramienta de codificación de IA	Conecta una herramienta de codificación de IA	No aplicable

Tarea	Registrarse en AWS (nuevo)	Registrarse en AWS (avanzado)
Eliminar todas las sesiones	Eliminar todas las sesiones en AWS Configuración	No aplicable
Excluya el uso de datos de IA	Opte por no usar su contenido para mejorar el servicio en AWS Configuración	Políticas de exclusión de servicios de IA
Solicitar los datos del	Solicita tu AWS Datos de identificación del constructor	Solicita tus datos
Elimina tu AWS perfil	Cierra tu cuenta en AWS Configuración	Cerrar un Cuenta de AWS
Administre las cuentas en India	Administre cuentas en India en AWS Configuración	Administre las cuentas en India
Creación de un usuario administrador	No aplicable	Registrarse en AWS (avanzado)
Planifique la estructura de gobierno de su cuenta	No aplicable	Planifica tu Cuenta de AWS estructura de gobierno

Registrarse en AWS (nuevo)

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Cuando utilizas Sign up for AWS (nuevo), creas un AWS entorno preconfigurado que te permite usar un nombre de usuario que ya tienes, como Google, o GitHub para acceder a tus AWS recursos. Los recursos se organizan en proyectos. Un proyecto contiene una configuración Cuenta de AWS y una configuración para compartirla con otros colaboradores. Si utilizas el plan de pago, tu proyecto también puede tener un coste mensual fijo antes de impuestos, denominado límite de gasto. Todos los proyectos que tienes forman parte de tu organización. Administras tu organización, accedes a tus proyectos y agregas miembros del equipo en AWS Configuración.


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

Cuando te registras para AWS usar Sign up for AWS (nueva), AWS también crea una ID de creador de AWS cuenta, que es un perfil personal que te representa como individuo. Solo puedes tener una ID de creador de AWS para cada dirección de correo electrónico. Si has creado una ID de creador de AWS pero no has creado ninguna Cuenta de AWS, es posible que ya tengas algunos ajustes configurados y que tengas que modificarlos más adelante.

Para obtener más información sobre la opción Registrarse en AWS (nueva), consulta la siguiente documentación:

- Compara las opciones de registro
- compatible Servicios de AWS para Inscríbase en AWS (nuevo)

Inscríbase mediante Registrarse para AWS (nuevo)

Cuando te inscribas AWS, es posible que te solicitemos información de pago. Nuestro proceso de verificación retiene 1 USD (o su equivalente) durante 3 a 5 días para verificar tu cuenta y evitar el fraude. No se te cobrará nada hasta que cambies a un plan de pago. Puedes administrar tu método de pago o cerrar tus cuentas en cualquier momento a través de la AWS Configuración. Además, al registrarte AWS, es posible que no cumplas los requisitos para la capa gratuita. En ese caso, tendrás que proporcionar tu información de pago y pasarás a formar parte del plan de pago. Cuando estás en el plan de pago, puedes establecer límites de gasto para operar dentro de un presupuesto predecible y controlado.

Inscríbete para obtener AWS (nuevas) ayudas con Google GitHub, Apple o Amazon para tu cuenta. Si ya has iniciado sesión en una cuenta de Google en el navegador, esa cuenta se utilizará cuando te registres AWS.

Para registrarte en AWS usando Registrarse para AWS (nuevo)

1. Abra la página Inscribirse en AWS.
2. Introduce tu correo electrónico o elige un nombre de usuario como Google GitHub, Apple o Amazon.
3. Si utilizas un nombre de usuario que ya tienes, se te redirigirá al nombre de usuario de tu proveedor. Después de iniciar sesión, se te redirigirá para que te AWS registres.
4. Introduce tu nombre y selecciona Continuar.

   Este nombre se comparte con los miembros del equipo cuando les das acceso a tus proyectos.

5. Verifica el correo electrónico asociado a tu inicio de sesión introduciendo un código de verificación. Cuando hayas verificado tu correo electrónico, selecciona Continuar.

   Este correo electrónico se comparte con los miembros del equipo cuando les das acceso a tus proyectos.

6. Introduce una contraseña segura para tu cuenta y selecciona Continuar.

   AWS requiere que la contraseña cumpla las siguientes condiciones:

   - Debe tener 8 caracteres como mínimo y 128 como máximo.
   - Debe incluir, como mínimo, tres de estos tipos de caracteres combinados: mayúsculas, minúsculas, números y símbolos ! @ # $ % ^ & * () <> [] {} | _+-=.
   - No debe ser idéntica a su Cuenta de AWS nombre o dirección de correo electrónico.

7. Introduce tus datos de contacto y selecciona Continuar.
8. AWS asignará un nombre nuevo a su primer proyecto de uno de los tres Regiones de AWS . Para obtener más información, consulte Regiones de AWS para tus proyectos. Puede cambiar el nombre en cualquier momento.

Ahora puede acceder al Consola de administración de AWS. Para acceder a AWS la configuración, elija Administrar proyectos en Consola de administración de AWS. En AWS Configuración, puedes invitar a miembros del equipo, crear nuevos proyectos y modificar la facturación y otros ajustes.

Siguientes pasos

Una vez que te hayas registrado AWS, podrás conectar una herramienta de programación de IA, añadir miembros del equipo para que colaboren y, si tienes un plan de pago, crear un límite de gasto.

- Conecta una herramienta de codificación de IA
- Invita a los miembros del equipo a colaborar en AWS Configuración
- Crea un límite de gasto en AWS Configuración

Uso AWS Configuración

> **Warning**
>
> Estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

AWSLa configuración es el lugar donde administras tus proyectos y accedes a ellos. AWS La configuración está disponible cuando te registras con Sign up for AWS (new). Puedes usar AWS la configuración para hacer lo siguiente:

- Crea proyectos de tu propiedad y accede a ellos. Para obtener más información, consulte Crea un proyecto en AWS Configuración.
- Accede a los proyectos que se han compartido contigo.
- Invita a los miembros del equipo a colaborar en tus proyectos. Para obtener más información, consulte Invita a los miembros del equipo a colaborar en AWS Configuración.
- Cambia de un proyecto a otro. Para obtener más información, consulte Cambiar entre proyectos.
- Gestiona tu método de pago. Para obtener más información, consulte Gestiona tu método de pago en AWS Configuración.
- Cambia de la capa gratuita a un plan de pago. Para obtener más información, consulte Actualiza tu cuenta en AWS Configuración.
- Gestiona los límites de gasto de tus proyectos. Para obtener más información, consulte Crea un límite de gasto en AWS Configuración.
- Consulta tu información de facturación. Para obtener más información, consulte Consulta tu información de facturación en AWS Configuración.
- Administra la información de tu perfil. Para obtener más información, consulte Gestiona tu nombre o apodo en AWS Configuración, Cambia tu dirección de correo electrónico en AWS Configuración y Edita tu información de contacto en AWS Configuración.
- Gestiona tu configuración de seguridad y tus preferencias de inicio de sesión. Para obtener más información, consulte Actualiza tu contraseña en AWS Configuración y Gestione la autenticación multifactor (MFA) en AWS Configuración.

Cuando administres la información de tu perfil o la configuración de seguridad, se te redirigirá al ID de creador de AWS hub. ID de creador de AWS El tuyo se crea cuando utilizas Registrarse en AWS (nuevo). Para obtener más información, consulta ¿Qué es ID de creador de AWS? .

Conecta una herramienta de codificación de IA

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Puedes proporcionar a tu herramienta de codificación de IA acceso a tu proyecto e instalar el kit de herramientas para agentes, que incluye la configuración del servidor AWS MCP y un conjunto de habilidades seleccionadas para los agentes. Esto permite que tu herramienta de codificación de IA cree y gestione AWS recursos en tu nombre.

Consideraciones para conectar tu herramienta de codificación a tu proyecto

- Puedes conectar las herramientas de codificación de IA a un proyecto de tu propiedad o a un proyecto que se haya compartido contigo.
- Cuando una herramienta de codificación de IA o un agente local crea AWS recursos, tú sigues siendo responsable de ellos. Esto incluye la seguridad adecuada de tus recursos, tal como se define en el modelo de responsabilidad compartida, así como cualquier cargo que puedan derivarse de estos recursos, tanto si se contabilizan en el plan gratuito como si se cobran en el plan de pago.
- Eres responsable de cualquier acción que tu herramienta de codificación de IA lleve a cabo en tu nombre en tus proyectos.
- Para ver un recurso que ha creado tu agente, ve a la consola de servicio de ese servicio.
- Las credenciales que genere son para que las usen los SDK AWS CLI PowerShell, AWS las herramientas y AWS los SDK. Es posible que las herramientas externas no sean compatibles. El acceso a sus recursos es válido durante 12 horas. Use el siguiente comando para renovar sus credenciales:

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

*profile-name*Sustitúyalas por el nombre de perfil que elegiste durante la configuración inicial. El comando abrirá automáticamente tu navegador predeterminado. Deberás elegir el nombre de tu proyecto para finalizar el proceso de inicio de sesión. AWS puede renovar sus credenciales durante 90 días. Después de 90 días, tendrás que volver a conceder el acceso en una ventana del navegador.

Conecta tu herramienta de codificación de IA a tu proyecto

Cada proyecto tiene su propio conjunto de credenciales que las herramientas de codificación de IA pueden usar para crear y administrar AWS recursos en tu nombre.

Consola de administración de AWS

Para conectar tu herramienta de codificación de IA a tu proyecto, utiliza el AWS consola

1. Abre AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, elige el proyecto al que deseas acceder.
3. En la barra de navegación de la esquina superior derecha, elija Crear y administrar la infraestructura de nube.
4. Selecciona Usa tus AWS credenciales con herramientas de codificación de IA.
5. Seleccione Copiar el mensaje del agente e introdúzcalo en su agente de codificación.

   Esto crea un mensaje que comparte un archivo de dirección con tu agente de codificación de IA. El archivo de dirección accede a un script desde el AWS que se establece la conexión entre las credenciales del proyecto y el agente de codificación de IA.

   Introducirás un nombre de perfil para tu proyecto. Este nombre de perfil indica cómo tu herramienta de codificación de IA accede a tus recursos.

Use your terminal

Ejecuta el siguiente comando para descargar y seguir las instrucciones de configuración:

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

Cuando utilices nuestra nueva AWS experiencia, tu agente instalará el servidor AWS MCP y tú tendrás acceso a las habilidades de agente que podrás utilizar en tus proyectos. También recibirá un archivo de reglas con instrucciones adaptadas a esta experiencia. El archivo de reglas también le permitirá definir el nivel de ayuda que desea que le brinde el agente. Los siguientes son los niveles de ayuda compatibles:

- Bajo: mientras construyes, la habilidad solo detectará los riesgos de seguridad. No sugerirá ninguna mejora o alternativa a tu arquitectura.
- Medio: mientras construyes, la habilidad puede hacerte algunas preguntas aclaratorias si detecta posibles problemas. No sugerirá ninguna mejora o alternativa a tu arquitectura.
- Alto: mientras construyes, la habilidad te proporcionará un alto nivel de apoyo. Te sugerirá mejoras o alternativas a tu arquitectura.

Trabaja con varios proyectos

Cada proyecto tiene su propio conjunto de credenciales que las herramientas de codificación de IA pueden usar para crear y administrar AWS recursos en tu nombre. Los perfiles se utilizan para acceder a cada proyecto. Un perfil es un archivo de credenciales y ajustes de configuración mantenido por el AWS CLI, y a cada perfil se le asigna un nombre único.

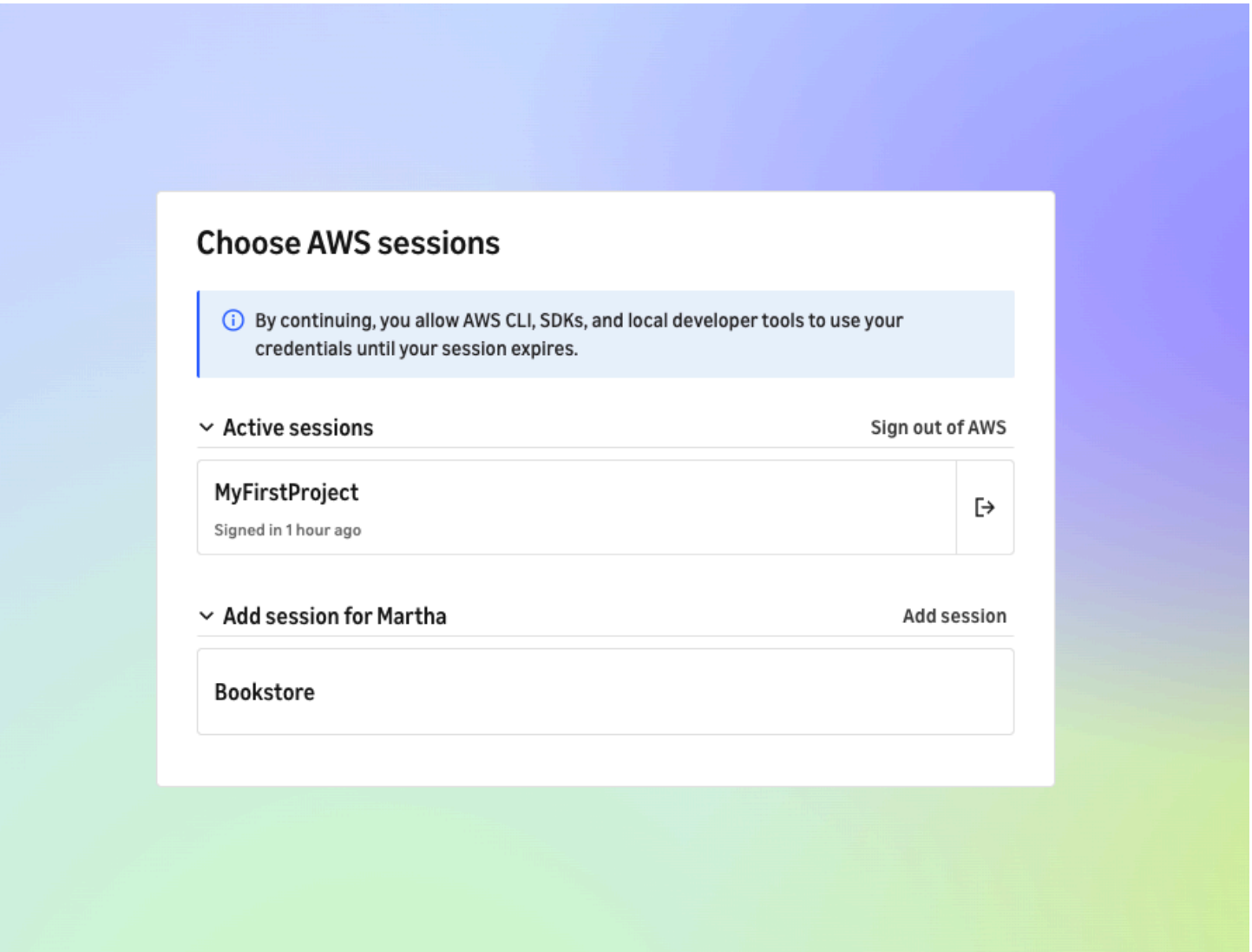
Por ejemplo, si tu primer proyecto fue `MyFirstProject` y elegiste el nombre del perfil `MyFirstProjectProfile` durante la configuración, puedes acceder a ese proyecto iniciando sesión en él AWS CLI con el siguiente comando:

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

Si creas otro proyecto con este nombre`Bookstore`, puedes acceder a él mediante el script de configuración y creando el perfil`BookstoreProfile`. A continuación, puede iniciar sesión en el AWS CLI con el siguiente comando:

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

Sin embargo, cuando ejecutes cualquiera de estos comandos, tendrás que elegir una sesión para tus AWS credenciales en la página Elegir AWS sesiones.



Esta página muestra las sesiones activas y las sesiones que puede agregar. Una sesión representa su estado de autenticación con sus AWS credenciales y proporciona las mismas credenciales que usa su agente de codificación de IA para crear y administrar los recursos.

En este ejemplo, ya ha iniciado sesión `MyFirstProject` y aún no lo ha hecho. `Bookstore` En la página Elegir AWS sesiones, puede hacer lo siguiente:

- Para seguir usando AWS for`MyFirstProject`, elija`MyFirstProject`.
- Para acceder`Bookstore`, elija`Bookstore`.
- Para eliminar cualquiera de las sesiones actuales, elija el icono de salida.
- Para acceder a un usuario de IAM que esté Cuenta de AWS utilizando, como una cuenta con la que hayas creadoRegistrarse en AWS (avanzado), selecciona Añadir sesión.

Las credenciales que elijas serán las mismas que usa tu agente de codificación de IA para crear y administrar recursos. Por ejemplo, puede iniciar sesión AWS CLI con el siguiente comando:

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

Si luego eliges la `Bookstore` sesión, tu herramienta de codificación de IA creará AWS recursos en el `Bookstore` proyecto.

Elige siempre la sesión que coincida con el proyecto asociado a tu perfil.

AWS acciones para los propietarios de proyectos

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Cuando eres el propietario de tu proyecto, tienes el control administrativo del proyecto. Esto incluye las tareas que puedes completarUso AWS Configuración. También tiene la posibilidad de realizar acciones exclusivas para usuarios root. Los miembros de tu equipo no pueden completar estas acciones.

Las acciones actuales que solo puedes realizar son las siguientes:

- Edita o elimina una política de bucket de S3 que deniega a todos los principales. Puede hacerlo para desbloquear un bucket de S3 con una política de bucket mal configurada.
- Edite o elimine una política basada en recursos de SQS que deniega a todos los principales. Puede hacerlo para desbloquear una cola de SQS con una política basada en recursos mal configurada.

Para realizar una acción que solo afecta a la raíz

1. Inicie sesión en su proyecto y abra la consola de IAM en. https://console.aws.amazon.com/iam/
2. En el panel de navegación de la consola de, elija Administración de acceso raíz.
3. Para la acción con privilegios, elija la acción con privilegios que desea realizar en la cuenta de miembro.

- Seleccione Eliminar política de bucket de Amazon S3 para eliminar una política de bucket mal configurada que impida a todas las entidades principales acceder al bucket de Amazon S3.

  a. Introduce la URI de S3 o elige Explorar S3 para seleccionar un nombre de entre los grupos de tu proyecto.

  b. Elija Eliminar política de bucket.

  c. Use la consola de Amazon S3 para corregir la política de bucket después de eliminar la política mal configurada. Para obtener más información, consulte Agregar una política de bucket mediante la consola de Amazon S3 en la Guía del usuario de Amazon S3.

- Seleccione Eliminar la política de Amazon SQS para eliminar una política basada en recursos que impide a todos los principales acceder a una cola de Amazon SQS.

  a. Introduzca el nombre de la cola en el nombre de la cola de SQS.

  b. Elija Eliminar la política de SQS.

  c. Use la consola de Amazon SQS para corregir la política de cola después de eliminar la política mal configurada. Para obtener más información, consulte Configuring an access policy in Amazon SQS en la Guía para desarrolladores de Amazon SQS.

Actualiza tu contraseña en AWS Configuración

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Puedes actualizar tu contraseña en AWS Configuración.

Para actualizar tu contraseña, visita AWS Configuración

1. Abre AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, elige Administrar la seguridad y el inicio de sesión.

   Se te redirigirá a tu perfil de AWS Builder ID.
3. Para la autorización, selecciona Actualizar contraseña.

4. En Current password (Contraseña actual), escriba la contraseña actual.
5. En Contraseña nueva, introduce una contraseña nueva.

   AWS requiere que la contraseña cumpla las siguientes condiciones:

   - Debe tener 8 caracteres como mínimo y 128 como máximo.
   - Debe incluir, como mínimo, tres de estos tipos de caracteres combinados: mayúsculas, minúsculas, números y símbolos ! @ # $ % ^ & * () <> [] {} | _+-=.
6. En Confirmar la nueva contraseña, introduce la nueva contraseña.
7. Elija Actualizar.

Gestione la autenticación multifactor (MFA) en AWS Configuración

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Multi-factor la autenticación (MFA) es un mecanismo simple y eficaz para mejorar su seguridad. El primer factor, su contraseña, es un secreto que debe memorizar, también conocido como factor de conocimiento. Otros factores pueden ser factores de posesión (algo que posea, como una clave de seguridad) o factores inherentes (algo que sea suyo y solo suyo, como un escaneo biométrico). Le recomendamos encarecidamente que configure la MFA para añadir una capa adicional a su cuenta.

Puede registrar un autenticador integrado y también una clave de seguridad que guarde en un lugar físico seguro. Si no puede utilizar el autenticador integrado, puede utilizar su clave de seguridad registrada. En el caso de las aplicaciones de autenticación, también puede habilitar la característica de copia de seguridad o sincronización en la nube en esas aplicaciones. Este sistema lo ayuda a evitar que pierda el acceso a su perfil si extravía su dispositivo MFA o este se rompe.

Puntos clave

Tenga en cuenta los siguientes puntos clave al registrar y administrar los dispositivos MFA:

- Le recomendamos que registre varios dispositivos MFA. Si pierdes el acceso a todos los dispositivos MFA registrados, no podrás recuperar tu cuenta.

- Le recomendamos que revise periódicamente sus dispositivos MFA registrados para asegurarse de que están actualizados y funcionan. Además, debe guardar esos dispositivos en un lugar que sea físicamente seguro cuando no los utilice.
- Si creó su cuenta mediante Continuar con Google, puede habilitar la autenticación multifactorial a través de su cuenta de Google. Para obtener más información, consulte Cómo activar la verificación en dos pasos.
- Si creaste tu cuenta con Continuar con Apple, es probable que la autenticación multifactorial ya esté habilitada en tu cuenta de Apple. De lo contrario, para obtener más información sobre cómo activarla, consulta la Two-factor autenticación de la cuenta de Apple.
- Si creaste tu cuenta con Continuar con GitHub, puedes habilitar la autenticación multifactorial a través de tu GitHub cuenta. Para obtener más información, consulte Configurar (GitHub) la autenticación de dos factores.
- Si creaste tu cuenta con Continue with Amazon, puedes activar la autenticación multifactorial a través de tu cuenta de Amazon. Para obtener más información, consulta ¿Qué es la Two-Step verificación? .

Tipos de MFA disponibles para nuestro nuevo AWS experiencia

Nuestra nueva AWS experiencia admite los siguientes tipos de dispositivos de autenticación multifactor (MFA).

Autenticadores FIDO2

El FIDO2 es un estándar que incluye el CTAP2 WebAuthny se basa en la criptografía de clave pública. Las credenciales FIDO son eficaces ante intentos de suplantación de identidad porque son exclusivas del sitio web en el que se crearon, por ejemplo AWS.

AWS admite los dos factores de forma más comunes para los autenticadores FIDO: los autenticadores integrados y las claves de seguridad. Consulte la sección que aparece a continuación para obtener más información sobre los tipos más comunes de autenticadores FIDO.

Built-in autenticadores

Algunos dispositivos tienen autenticadores integrados, como TouchID MacBook o una cámara de Windows. Hello-compatible Si tu dispositivo es compatible con los protocolos FIDO, por ejemplo WebAuthn, puedes usar tu huella digital o tu rostro como segundo factor. Para obtener más información, consulte Autenticación FIDO.

Claves de seguridad

Puedes comprar una llave USB, BLE o de NFC-connected seguridad FIDO2-compatible externa. Cuando se te pida un dispositivo MFA, toca el sensor de la tecla. YubiKey o Feitian fabrica dispositivos compatibles. Para obtener una lista de todas las llaves de seguridad compatibles, consulte los Productos certificados por FIDO.

Administradores de contraseñas, proveedores de claves de acceso y otros autenticadores FIDO

Existen varios proveedores externos que admiten la autenticación FIDO en las aplicaciones móviles, como características disponibles en administradores de contraseñas, tarjetas inteligentes con modo FIDO y otros formatos. Estos FIDO-compatible dispositivos pueden funcionar con IAM Identity Center, pero le recomendamos que pruebe usted mismo un autenticador FIDO antes de activar esta opción para MFA.

> **Note**
>
> Algunos autenticadores FIDO pueden crear credenciales FIDO reconocibles, conocidas como claves de acceso. Las claves de acceso pueden estar vinculadas al dispositivo que las crea o pueden sincronizarse y guardarse copias de seguridad en una nube. Por ejemplo, se puede registrar una clave de acceso con el Apple Touch ID en un MacBook compatible y, a continuación, iniciar sesión en un sitio desde un portátil Windows con Google Chrome con la clave de acceso en iCloud siguiendo las instrucciones que aparecen en pantalla al iniciar sesión. Para obtener más información sobre qué dispositivos admiten claves de acceso sincronizables y la interoperabilidad actual de claves entre sistemas operativos y navegadores, consulte Asistencia para dispositivos en passkeys.dev, un recurso proporcionado por la Alianza FIDO y el Consorcio World Wide Web (W3C).

Aplicaciones de autenticación

Las aplicaciones de autenticación son autenticadores de terceros basados en contraseñas de un solo uso (OTP). Puede utilizar una aplicación de autenticación instalada en su dispositivo móvil o tableta como dispositivo MFA autorizado. La aplicación de autenticación de terceros debe cumplir con RFC 6238, que es un algoritmo de contraseña temporal de un solo uso (TOTP) basado en estándares y capaz de generar códigos de autenticación de seis dígitos.

Cuando se le pida la MFA, debe introducir un código válido de su aplicación de autenticación en el cuadro de entrada que aparece. Cada dispositivo MFA asignado a un usuario debe ser único. Se pueden registrar dos aplicaciones de autenticación para un usuario determinado.

Puede elegir entre las siguientes aplicaciones de autenticación de terceros conocidas. Sin embargo, cualquier TOTP-compliant aplicación funciona con AWS Builder ID MFA.

Sistema operativo	Aplicación de autenticación probada
Android	1Password, Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator
iOS	1Password, Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator

Registrar su dispositivo MFA de

> **Note**
>
> Después de registrar una MFA, cerrar sesión e iniciar sesión en el mismo dispositivo, es posible que no se le pida una MFA en dispositivos de confianza.

Para registrar su dispositivo MFA mediante una aplicación de autenticación

1. Abra la AWS configuración en. https://settings.aws.com
2. En el panel de navegación principal, selecciona Administrar la seguridad y el inicio de sesión.

   Se te redirigirá a tu perfil de AWS Builder ID.
3. En la página Seguridad, seleccione Registrar dispositivo.
4. En la página Registrar dispositivo MFA, elija la App Authenticator.
5. AWS Builder ID funciona y muestra información de configuración, incluido un gráfico de código QR. El gráfico es una representación de la “clave de configuración secreta” que se puede introducir manualmente en aplicaciones de autenticación que no admiten códigos QR.
6. Abra su aplicación de autenticación. Para obtener una lista de aplicaciones, consulte Aplicaciones de autenticación.

Si la aplicación de autenticación admite varios dispositivos o cuentas de MFA, elija la opción de crear un nuevo dispositivo o cuenta de MFA virtual.

7. Determine si la aplicación de MFA admite códigos QR y, a continuación, lleve a cabo alguna de las siguientes operaciones en la página Aplicación para configurar un autenticador

   1. Elija Mostrar código QR y, a continuación, utilice la aplicación para escanear el código QR. Por ejemplo, puede elegir el icono de la cámara o una opción similar a Escanear código. A continuación, use la cámara del dispositivo para escanear el código.
   2. Seleccione Mostrar clave secreta y, a continuación, introduzca esa clave secreta en su aplicación de MFA.

   Cuando termine, la aplicación de autenticación generará y mostrará una contraseña de un solo uso.

8. En el cuadro del Código de autenticación, introduzca la contraseña de un solo uso que aparece actualmente en la aplicación de autenticación. Elija Asignar MFA.

   > **Important**
   >
   > Envíe su solicitud inmediatamente después de generar el código. Si generas el código y esperas demasiado para enviar la solicitud, el dispositivo MFA se asociará correctamente a tu AWS Builder ID, pero el dispositivo MFA no estará sincronizado. Esto ocurre porque las contraseñas temporales de un solo uso (TOTP) caducan tras un corto periodo de tiempo. Si esto ocurre, puede volver a sincronizar el dispositivo. Para obtener más información, consulte *I get the message 'An unexpected error has occurred' when I try to register or sign in with an authenticator app*.

9. Para asignar a tu dispositivo un nombre descriptivo en AWS Builder ID, selecciona Cambiar nombre. Este nombre lo ayuda a distinguir este dispositivo de los demás que registre.

El dispositivo MFA ya está listo para usarse con AWS Settings, sus proyectos y AWS Builder ID.

Registrar una clave de seguridad como dispositivo MFA de

Para registrar su dispositivo MFA mediante una clave de seguridad

1. Abra la AWS configuración en. https://settings.aws.com
2. En el panel de navegación principal, selecciona Administrar la seguridad y el inicio de sesión.

   Se te redirigirá a tu perfil de AWS Builder ID.
3. En la página Seguridad, seleccione Registrar dispositivo.
4. En la página Registrar dispositivo MFA, elija Clave de seguridad.
5. Asegúrese de que su clave de seguridad esté habilitada. Si utiliza una clave de seguridad física independiente, conéctela a su equipo.
6. Siga las instrucciones que aparecen en pantalla. Los pasos cambian según el sistema operativo y el navegador.
7. Para asignar a tu dispositivo un nombre descriptivo en AWS Builder ID, selecciona Cambiar nombre. Este nombre lo ayuda a distinguir este dispositivo de los demás que registre.

El dispositivo MFA ya está listo para usarse con AWS Settings, sus proyectos y AWS Builder ID.

Cambie el nombre del dispositivo MFA de

Para cambiar el nombre del dispositivo MFA

1. Abra la AWS configuración en. https://settings.aws.com
2. En el panel de navegación principal, selecciona Administrar la seguridad y el inicio de sesión.

   Se te redirigirá a tu perfil de AWS Builder ID.
3. Elija Seguridad. Cuando llegue a la página, verá que Cambiar nombre aparece atenuado.
4. Seleccione el dispositivo MFA que desea cambiar. Esto le permite elegir Cambiar nombre. A continuación, aparece un cuadro de diálogo.
5. En el mensaje que se abre, introduzca el nuevo nombre en Nombre del dispositivo MFA y elija Cambiar nombre. El dispositivo al que se le ha cambiado el nombre aparece en los dispositivos de Multi-factor autenticación (MFA).

Eliminar su dispositivo MFA

Se recomienda mantener dos o más dispositivos MFA activos. Para deshabilitar la autenticación multifactor, elimine todos los dispositivos MFA registrados de su perfil.

Para eliminar un dispositivo MFA

1. Abre los AWS ajustes en. https://settings.aws.com
2. En el panel de navegación principal, selecciona Administrar la seguridad y el inicio de sesión.

   Se te redirigirá a tu perfil de AWS Builder ID.
3. En la página Seguridad, seleccione el dispositivo de MFA que desee cambiar y elija Eliminar.
4. En la sección ¿Eliminar dispositivo MFA?, siga las instrucciones para eliminar su dispositivo.
5. Elija Eliminar.

El dispositivo eliminado ya no aparece en los dispositivos de Multi-factor autenticación (MFA).

Eliminar todas las sesiones en AWS Configuración

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Puedes eliminar todas las sesiones de todos los dispositivos en AWS Configuración. Si hay un dispositivo que no reconoces, cambia la contraseña y elimina todas las sesiones.

Para eliminar todas las sesiones

1. Abra AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, elige Administrar la seguridad y el inicio de sesión.

   Se te redirigirá a tu perfil de AWS Builder ID.
3. En los dispositivos con sesión iniciada, selecciona Eliminar todas las sesiones.
4. Confirma tu elección y elige Eliminar todas las sesiones.

Se cerrará la sesión de AWS Configuración.

Gestiona tu nombre o apodo en AWS Configuración

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Puedes cambiar tu nombre en cualquier momento. Todos los miembros del equipo pueden ver tu nombre y, si te has cambiado al plan de pago, este es el nombre que aparece en la información de facturación. Si te suscribiste AWS en la India, tu nombre debe coincidir exactamente con el nombre que aparece en el documento que planeas usar para la verificación del cliente.

Cuando cambias tu nombre, cambias el nombre que aparece en tu ID de AWS constructor. Esto afectará a tu nombre en la AWS Configuración, a tu ID de AWS Constructor y a cualquier AWS recurso al que accedas directamente a través del ID de AWS Constructor.

Tu nombre hace referencia a ti en las herramientas y los servicios cuando interactúas con otras personas. Tu apodo indica cómo quieres que te conozcan tus amigos y otras personas con las que colaboras estrechamente. AWS

Para cambiar tu nombre o apodo

1. Abre AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Administrar perfil.
3. Para ver la información del perfil, selecciona Administrar perfil.

   Se te redirigirá a tu perfil de AWS Builder ID.
4. Para obtener información sobre el perfil, selecciona Editar.
5. (Opcional) En Nombre, introduce un nombre nuevo.
6. (Opcional) Para el apodo, introduce un apodo nuevo.
7. Seleccione Save changes (Guardar cambios).

Cambia tu dirección de correo electrónico en AWS Configuración

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Puedes cambiar tu correo electrónico en AWS Configuración. Cuando cambies tu correo electrónico, el correo anterior se separará de tu AWS perfil y de tu ID de AWS creador. No podrás usar ese correo electrónico para acceder a ninguno de los proyectos de AWS Configuración, pero puedes usarlo para AWS volver a registrarte.

Tu dirección de correo electrónico se comparte con los miembros del equipo cuando les das acceso a tus proyectos.

Para cambiar tu correo electrónico

1. Abre AWS Configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Administrar perfil.
3. Para ver la información del perfil, selecciona Administrar perfil.

   Se te redirigirá a tu perfil de AWS Builder ID.
4. Para ver la información de contacto, selecciona Editar.
5. En Dirección de correo electrónico, introduce una nueva dirección de correo electrónico y selecciona Verificar correo electrónico. Te enviaremos un código de verificación para tu nueva dirección de correo electrónico. Lo introducirás en el cuadro emergente de verificación del correo electrónico.
6. Para el código de verificación, introduce el código de verificación que te enviamos a tu nuevo correo electrónico.
7. Seleccione Verificar.

Edita tu información de contacto en AWS Configuración

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Puedes editar el número de teléfono o la dirección asociados a AWS la configuración. Al modificar estos valores, es posible que afecten a las obligaciones tributarias.

Para editar la información de contacto

1. Abre AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Administrar perfil.
3. Para la información de contacto, selecciona Editar.
4. Ingresa la nueva información de contacto.
5. Seleccione Save.

Opte por no usar su contenido para mejorar el servicio en AWS Configuración

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

AWS Los servicios de IA pueden usar y almacenar el contenido de los clientes para mejorar el servicio, como solucionar problemas operativos, evaluar el rendimiento del servicio, depurar errores o capacitar a los modelos. Con este fin, es posible que almacenemos dicho contenido en un lugar Región de AWS externo al Región de AWS lugar en el que utilizas el servicio. Puedes inhabilitar el uso de tu contenido para mejorar el servicio a través de AWS la Configuración. El efecto de la exclusión voluntaria es que tu AWS organización aplica AWS una política de exclusión voluntaria de los servicios de IA. Para obtener más información sobre las políticas de exclusión voluntaria, consulta la documentación sobre las políticas de exclusión de los servicios de IA.

Si optas por excluirte de todos los servicios, todos tus proyectos quedarán excluidos de las mejoras del servicio y utilizarán tu contenido para los servicios de IA compatibles actuales y futuros, respaldados por las políticas de exclusión de los servicios de IA.

Es necesario tomar medidas adicionales para excluirse de Amazon Monitron. Para obtener más información, consulte los Términos del servicio de AWS. Solo el propietario del proyecto puede inhabilitar el uso de datos por parte de los servicios de AWS IA.

Para excluirse del uso de datos: AWS Servicios de IA

1. Abra AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, elija Proyecto.
3. En Descripción general, seleccione Acciones y, a continuación, elija Excluir el uso de datos por parte de los servicios de AWS IA.
4. Confirme su elección y elija Excluirse.

Solicita tu AWS Datos de identificación del constructor

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Puedes solicitar y ver la información personal asociada a tu ID de AWS Builder y a las AWS aplicaciones y servicios a los que accediste con tu ID de AWS Builder. Procesaremos su solicitud en un plazo de 30 días y le notificaremos cuando sus datos estén listos. Mientras tu solicitud de datos esté pendiente, no podrás cerrar tu AWS perfil. Aún puedes cerrar los proyectos o la organización propietaria de todos tus proyectos.

Para obtener más información sobre el ejercicio de sus derechos como titular de los datos, incluida la información personal proporcionada en relación con otros AWS sitios web, aplicaciones, productos, servicios, eventos y experiencias, consulte AWS Privacidad.

Para solicitar sus datos

1. Abre AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Administrar perfil.

3. Selecciona Administrar perfil.

   Se te redirigirá a tu perfil de AWS Builder ID.
4. Seleccione Privacidad y datos.
5. Elige solicitar tus datos de Builder ID o tus AWS datos.

   Aparece un mensaje de confirmación verde en la parte superior de la página en el que se indica que hemos recibido su solicitud y que la completaremos en un plazo de 30 días.
6. Cuando recibas un correo electrónico de nuestra parte informándote de que la solicitud se ha procesado, vuelve a la página de privacidad y datos de tu perfil de AWS Builder ID. Seleccione el nuevo botón disponible Descargar archivo ZIP con sus datos.

Mientras tu solicitud de datos esté pendiente, no podrás eliminar tu ID de AWS Builder.

Crea un proyecto en AWS Configuración

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Un proyecto contiene una única en la Cuenta de AWS que se crean AWS recursos. Un proyecto también incluye ajustes para compartirlos con otros colaboradores. Los AWS recursos que crees deben representar una aplicación o un conjunto de casos de uso relacionados. Un proyecto puede abarcar los entornos de desarrollo y producción de su aplicación. Por ejemplo, puede crear un proyecto denominado Librería que contenga recursos para una aplicación de librería, como una base de datos, recursos informáticos y almacenamiento.

Puedes compartir este proyecto con otros miembros del equipo, y ellos pueden crear y administrar los recursos para la aplicación de librería.

Cada proyecto tiene sus propios controles de costes en función de los recursos de la cuenta. Si utilizas el plan de pago, puedes configurar un límite de gasto en los AWS ajustes para cada proyecto. Para obtener más información, consulte Crea un límite de gasto en AWS Configuración. Como propietario del proyecto, eres responsable de las facturas mensuales de los cargos por uso y las tarifas recurrentes.

Consideraciones para crear un proyecto

- Como miembro del equipo, puedes acceder a proyectos que no son de tu propiedad.
- El nombre de cada proyecto debe ser único para tus proyectos. Los proyectos propiedad de otros miembros del equipo pueden tener el mismo nombre.
- Los nombres de los proyectos pueden contener los siguientes caracteres válidos: a-z A-Z, 0-9 y puntos (.).
- Cuando crees tu proyecto, AWS asígnalo a una región (EE. UU. Este (Ohio) (`us-east-2`), Europa (Estocolmo) (`eu-north-1`) o Asia Pacífico (Sídney) (`ap-southeast-2`), en función del país de tu dirección de contacto, ya sea Estados Unidos, Europa o Asia Pacífico. Todos los recursos regionales que crees se alojarán en esa región. Para obtener más información, consulte Regiones de AWS para tus proyectos.

Para crear un proyecto

Para crear un proyecto

1. Abre AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, elija Proyecto.
3. Elija Crear proyecto.
4. En Nombre del proyecto, introduzca un nombre descriptivo para el proyecto.

   Este nombre se comparte con los miembros del equipo cuando los invitas a colaborar.
5. Seleccione Crear.

La creación del proyecto tardará unos segundos. Cuando su proyecto esté disponible, podrá seleccionarlo y acceder a él Consola de administración de AWS para empezar a crear.

Si ya has configurado tu herramienta de programación de IA para que interactúe con la tuya Cuenta de AWS, puedes pedirle que cree recursos para tu nuevo proyecto.

Usa las instrucciones de ejemplo de tu herramienta de codificación de IA para empezar:

```
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.
```

Regiones de AWS para tus proyectos

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Cuando crees tu proyecto, AWS asígnalo a una región (EE. UU. Este (Ohio) (`us-east-2`), Europa (Estocolmo) (`eu-north-1`) o Asia Pacífico (Sídney) (`ap-southeast-2`)), según el país de tu dirección de contacto, ya sea Estados Unidos, Europa o Asia Pacífico. Todos los recursos regionales que crees se alojarán en esa región.

Las siguientes son consideraciones para los seleccionados Región de AWS para su cuenta:

- Si cambias tu información de contacto en AWS la configuración, la región seleccionada no cambiará. Si necesitas acceder a una región específica, usa la opción de registro AWS (avanzada). También puedes activar funciones avanzadas en tu cuenta para seleccionar diferentes regiones.
- AWS puede introducir regiones compatibles adicionales, pero solo estarán disponibles para los nuevos usuarios. Para ver las regiones compatibles más recientes, publicadas el 18 de agosto de 2026, consulta las tablas que aparecen a continuación. Si ya tienes un proyecto, puedes encontrar la región que has seleccionado en AWS Ajustes.
- Los servicios globales están disponibles con tu proyecto. Se accede a estos servicios a través de una única región que puede diferir de la de su región de origen. Para más información, consulte AWS Fault Isolation Boundaries. Además, hay algunos servicios que están disponibles en regiones específicas. En el Consola de administración de AWS, puede ver estos servicios en determinadas regiones, pero volverá a la región seleccionada cuando navegue a un servicio diferente.
- Si utiliza Amazon Bedrock, puede utilizar las API que no crean recursos en todos los anuncios Regiones de AWS que están habilitados de forma predeterminada.
- Si las utilizas CloudFront, algunas funciones que crearían recursos fuera de la región seleccionada no están disponibles. Esto incluye el uso AWS WAF con CloudFront.
- Algunos CloudTrail eventos relacionados con los servicios globales se registran en la región en la que opera el servicio global. Tienes acceso a estos eventos.

- AWS WAF y Amazon CloudWatch Logs está disponible en el este de EE. UU. (Virginia del Norte) (`us-east-1`).

Puedes averiguar cuál es la región seleccionada para todos los proyectos de tu cuenta en la AWS configuración. En Consola de administración de AWS, la mayoría de las consolas de servicio están alojadas en la región en la que te encuentras, incluidas Bedrock y SageMaker. Si alguna vez consultas una consola de servicio de un servicio global, la consola dirige automáticamente todas tus llamadas a la API a la región correspondiente para el servicio global.

Busca la seleccionada Región de AWS para tus proyectos

Como práctica recomendada, te recomendamos que siempre confirmes la Región de AWS para tu proyecto antes de crear cualquier AWS recurso.

Para encontrar el seleccionado Región de AWS para tus proyectos

1. Abre AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, elija Proyecto.
3. En la sección Descripción general, seleccione Información adicional.

   En esta vista, también puedes encontrar el Cuenta de AWS ID asociado a tu proyecto.
4. En el caso de la región, verás en qué se ha aprovisionado Región de AWS tu proyecto.

Cuando crees AWS recursos regionales en cualquiera de tus proyectos, los nombres de los recursos de Amazon de estos recursos incluirán este Región de AWS dato.

Países en los que se aprovisionan recursos regionales en el este de EE. UU. (Ohio) (us-east-2)

Country name (Nombre del país)	Código de país
Antigua y Barbuda	AG
Argentina	AR
Bahamas	BS

Country name (Nombre del país)	Código de país
Barbados	BB
Belice	BZ
Bolivia	BO
Brasil	BR
Canadá	CA
Chile	CL
Colombia	CO
Costa Rica	CR
Dominica	DM
República Dominicana	DO
Ecuador	EC
El Salvador	SV
Granada	GD
Guatemala	GT
Guyana	GY
Haití	HT
Honduras	HN
Jamaica	JM
México	MX
Nicaragua	NI

Country name (Nombre del país)	Código de país
Panamá	PA
Paraguay	PY
Perú	PE
San Cristóbal y Nieves	KN
Santa Lucía	LC
San Vicente y las Granadinas	VC
Surinam	SR
Trinidad y Tobago	TT
Estados Unidos	EE. UU.
Uruguay	UY
Venezuela	VE
Anguila	IA
Aruba	AW
Bermudas	BM
Bonaire, San Eustaquio y Saba	BQ
Islas Vírgenes Británicas	VG
Islas Caimán	KY
Curazao	CW
Islas Malvinas	FK
Guayana Francesa	GF

Country name (Nombre del país)	Código de país
Guadalupe	GP
Martinica	MQ
Montserrat	MS
Puerto Rico	PR
San Bartolomé	BL
San Martín (Francia)	MF
San Pedro y Miquelón	PM
San Martín (Países Bajos)	SX
Islas Turcas y Caicos	TC
U.S. Islas Vírgenes	VI

Países en los que se aprovisionan recursos regionales en Asia Pacífico (Sídney) (ap-southeast-2)

Country name (Nombre del país)	Código de país
Afganistán	AF
Australia	AU
Bangladesh	BD
Bután	BT
Brunéi	BN
Camboya	KH

Country name (Nombre del país)	Código de país
China	CN
Timor-LesteTimor Oriental ()	TL
Fiyi	FJ
Hong Kong	HK
India	IN
Indonesia	ID
Japón	JP
Kazajistán	KZ
Kiribati	KI
Kirguistán	KG
Laos	LA
Macao	MO
Malasia	MY
Maldivas	MV
Islas Marshall	MH
Micronesia	FM
Mongolia	MN
Myanmar	MM
Nauru	NR
Nepal	NP

Country name (Nombre del país)	Código de país
Nueva Zelanda	NZ
Pakistán	PK
Palaos	PW
Papúa Nueva Guinea	PG
Filipinas	PH
Samoa	WS
Singapur	SG
Islas Salomón	SB
Corea del Sur	KR
Sri Lanka	LK
Taiwán	TW
Tayikistán	TJ
Tailandia	TH
Tonga	TO
Turkmenistán	TM
Tuvalu	TV
Uzbekistán	UZ
Vanuatu	VU
Vietnam	VN
Samoa Americana	AS

Country name (Nombre del país)	Código de país
Isla de Navidad	CX
Islas Cocos	CC
Islas Cook	CK
Polinesia Francesa	PF
Guam	GU
Isla e McDonald islas Heard	HM
Nueva Caledonia	NC
Niue	NU
Isla Norfolk	NF
Islas Marianas del Norte	MP
Islas Pitcairn	PN
Tokelau	TK
U.S. Islas periféricas menores	UM
Wallis y Futuna	WF

Países en los que se aprovisionan recursos regionales en Europa (Estocolmo) (**`eu-north-1`**)

Country name (Nombre del país)	Código de país
Albania	AL
Argelia	DZ

Country name (Nombre del país)	Código de país
Andorra	AD
Angola	AO
Armenia	a. m.
Austria	AT
Azerbaiyán	AZ
Bahréin	BH
Bielorrusia	BY
Bélgica	BE
Benín	BJ
Bosnia y Herzegovina	BA
Botsuana	BW
Bulgaria	BG
Burkina Faso	BF
Burundi	BI
Cabo Verde	CV
Camerún	CM
República Centroafricana	CF
Chad	TD
Comoras	KM
Congo (Brazzaville)	CG

Country name (Nombre del país)	Código de país
Congo (RDC)	CD
Costa de Marfil	CI
Croacia	HR
Chipre	CY
República Checa	CZ
Dinamarca	DK
Yibuti	DJ
Egipto	EG
Guinea Ecuatorial	GQ
Eritrea	ER
Estonia	EE
Suazilandia	SZ
Etiopía	ET
Finlandia	FI
Francia	FR
Gabón	GA
Gambia	GM
Georgia	GE
Alemania	DE
Ghana	GH

Country name (Nombre del país)	Código de país
Grecia	GR
Guinea	GN
Guinea-Bissau	GW
Hungría	HU
Iceland	IS
Irak	IQ
Irlanda	IE
Israel	IL
Italia	TI
Jordania	JO
Kenia	KE
Kosovo	XK
Kuwait	KW
Letonia	LV
Líbano	LB
Lesoto	LS
Liberia	LR
Libia	LY
Liechtenstein	LI
Lituania	LT

Country name (Nombre del país)	Código de país
Luxemburgo	LU
Madagascar	MG
Malawi	MW
Mali	ML
Malta	MT
Mauritania	MR
Mauricio	MU
Moldavia	MD
Mónaco	MC
Montenegro	ME
Marruecos	MA
Mozambique	MZ
Namibia	N/D
Países Bajos	NL
Níger	NE
Nigeria	NG
Macedonia del Norte	MK
Noruega	NO
Omán	OM
Palestina	PS

Country name (Nombre del país)	Código de país
Polonia	PL
Portugal	PT
Catar	QA
Rumanía	RO
Rusia	RU
Ruanda	RW
San Marino	SM
Santo Tomé y Príncipe	ST
Arabia Saudí	SA
Senegal	SN
Serbia	RS
Seychelles	SC
Sierra Leona	SL
Eslovaquia	SK
Eslovenia	SI
Somalia	SO
Sudáfrica	ZA
Sudán del Sur	SS
España	ES
Suecia	SE

Country name (Nombre del país)	Código de país
Suiza	CH
Tanzania	TZ
Togo	TG
Túnez	TN
Turquía	TR
Uganda	UG
Ucrania	UA
Emiratos Árabes Unidos	AE
Reino Unido	GB
Ciudad del Vaticano	VA
Yemen	YE
Zambia	ZM
Zimbabue	ZW
Islas Åland	AX
Antártida	AQ
Isla Bouvet	BV
Territorio Británico del Océano Índico	E/S
Islas Faroe	FO
Territorios Australes Franceses	TF
Gibraltar	GI

Country name (Nombre del país)	Código de país
Groenlandia	GL
Guernsey	GG
Isla de Man	IM
Jersey	JE
Mayotte	YT
Reunión	RE
Santa Elena	SH
Islas Georgias del Sur y Sandwich del Sur	GS
Svalbard y Jan Mayen	SJ
Sahara Occidental	EH

Políticas gestionadas para su organización

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Al utilizar nuestra nueva AWS experiencia, AWS gestiona las políticas de gestión de la organización, incluidas las políticas de control de recursos (RCP) y las políticas de control de servicios (SCP). Estos controles de protección impiden que el propietario del proyecto o un miembro del equipo lleve a cabo acciones que puedan inhibir los valores predeterminados preconfigurados que se AWS han definido para ayudarle a crear y desarrollarse rápidamente.

Políticas de control de servicios para proyectos

La siguiente es una política de control de servicios para todos los usuarios de un proyecto y no se puede cambiar:

```
{
  "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"
        }
      }
```

```
    }
  ]
}
```

Esta política no se elimina al activar las funciones avanzadas. Para obtener más información, consulte Activar avanzado AWS Características de .

Una vez activadas las funciones avanzadas, esta política permanece vinculada a la raíz de la organización, por lo que se aplica a todas las cuentas de los miembros, incluidas las cuentas que cree o invite posteriormente.

Además, aplicamos la siguiente política de control de servicios a todos los usuarios de un proyecto para restringir determinadas modificaciones del proyecto que no se admiten o que deben realizarse en la AWS configuración:

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

Esta política se elimina al activar las funciones avanzadas. Para obtener más información, consulte Activar avanzado AWS Características de .

Si eliminas esta política, no podrás actualizar la dirección de correo electrónico del usuario raíz de una cuenta de proyecto. Para obtener más información, consulte Proyecte las cuentas después de activar las funciones avanzadas.

Además, también aplicamos la siguiente política de control de servicios a todos los usuarios de un proyecto para restringirla y Regiones de AWS permitir la compatibilidad con los servicios particionales, según tu *selected-region* perfil:

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

Tras activar las funciones avanzadas, se aplicará a tu cuenta la siguiente política de control de servicios:

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

```
}
```

Políticas de control de servicios para los límites de gasto

Si utilizas un límite de gasto, las siguientes políticas de control de servicios se aplicarán a tu proyecto a medida que se acerque al límite de gasto. Para obtener más información sobre los límites de gasto, consulteCrea un límite de gasto en AWS Configuración.

```
{
  "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": "*"
    }
  ]
}
```

Políticas de control de servicios para la capa gratuita para proyectos

La siguiente política de control de servicios controla el acceso a AWS los servicios disponibles en el nivel gratuito de nuestra nueva AWS experiencia. Esta política no se puede modificar. Para acceder a servicios adicionales, actualice su cuenta. Para obtener más información, consulte Actualiza tu cuenta en AWS Configuración.

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

Políticas de control de servicios para el plan de pago para proyectos

La siguiente política de control de servicios controla el acceso a AWS los servicios disponibles en el plan de pago de nuestra nueva AWS experiencia. Esta política no se puede modificar. Para acceder a servicios adicionales, active las funciones avanzadas. Para obtener más información, consulte Activar avanzado AWS Características de .

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

Políticas de control de recursos para proyectos

La siguiente es la política de control de recursos para los recursos del proyecto. Esta política no se puede modificar:

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

Cambiar entre proyectos

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Solo puedes administrar AWS los recursos de un proyecto a la vez. Siempre puedes saber en qué proyecto te encuentras en función del nombre que aparece en la esquina superior derecha de la AWS consola.

Cambia de un proyecto a otro para ver las sesiones activas desde la Consola de administración de AWS

Para cambiar de un proyecto a otro para las sesiones activas, desde Consola de administración de AWS

1. Abra la Consola de administración de AWS.
2. Elige el nombre de tu proyecto en la esquina superior derecha del Consola de administración de AWS.
3. Elige Switch project.

4. En Sesiones activas, elige una sesión activa. Una sesión activa es una sesión en la que se ha iniciado sesión durante un máximo de 12 horas. La hora de la sesión activa no se puede cambiar.
5. Se te redirigirá a la página de inicio de la AWS consola para tu nuevo proyecto.

Cambia de un proyecto a otro en AWS Configuración

Para cambiar entre proyectos en AWS Configuración

1. Abra AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, elige el proyecto al que deseas acceder.
3. En la barra de navegación de la esquina superior derecha, elija Crear y administrar la infraestructura de nube.

   Se te redirigirá de nuevo a la Consola de administración de AWS para tu nuevo proyecto.

Cambia de un proyecto a otro desde el Consola de administración de AWS

Para cambiar de un proyecto a otro desde Consola de administración de AWS

1. Abra la Consola de administración de AWS.
2. Elige Gestionar proyectos.
3. En AWS Configuración, elige el proyecto al que quieres acceder.
4. En la barra de navegación de la esquina superior derecha, selecciona Crear y gestionar la infraestructura de nube.

   Se te redirigirá de nuevo a la Consola de administración de AWS para tu nuevo proyecto.

Invita a los miembros del equipo a colaborar en AWS Configuración

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Puedes dar acceso a tus proyectos a los miembros del equipo. Cuando compartes un proyecto con un miembro del equipo, no puedes controlar a qué AWS servicios tiene acceso. Tanto tú como el miembro del equipo tenéis acceso de administrador al proyecto. Esto significa que el miembro del equipo tiene permisos para acceder a todos los AWS servicios disponibles para tu proyecto. Esto incluye la creación de controles de acceso para los servicios y las aplicaciones. Sin embargo, no tienen permisos para realizar acciones administrativas o financieras, como eliminar un proyecto o modificar un límite de gastos. Para ver qué miembro del equipo ha modificado un AWS servicio, consultaSupervise su proyecto mediante AWS CloudTrail.

En AWS Configuración, tú y los miembros de tu equipo tenéis diferentes niveles de acceso. Para ver la política AWS gestionada que se aplica a un miembro del equipo, consulta AWSManagedSettingsReadOnlyAccess. Para ver la política AWS gestionada que se aplica al propietario de un proyecto, consulte AWSManagedSettingsAdminAccess.

Tenga en cuenta lo siguiente cuando añada a un miembro del equipo a su proyecto.

Consideraciones para los miembros del equipo

Un miembro del equipo puede realizar las siguientes acciones:

- Ver, crear, editar, eliminar y modificar AWS los recursos de un proyecto.
- AWS Configuración de acceso.
- Consulta los límites de gasto.
- Solicita un aumento de cuota para un AWS servicio.

Un miembro del equipo no puede realizar las siguientes acciones:

- Abandonar un proyecto.
- Realiza cualquier acción de raíz. Para obtener más información, consulte AWS acciones para los propietarios de proyectos.
- Invita a los miembros del equipo a participar en los proyectos.
- Gestiona los permisos de cualquier miembro del equipo.
- Elimina a cualquier miembro del equipo de un proyecto.
- Cambia el nombre de un proyecto.
- Configura o actualiza los métodos de pago.
- Consulta o actualiza los detalles de facturación, incluidos la dirección o el número de teléfono.

- Ver o actualizar la información tributaria.
- Cambie de un plan gratuito a un plan de pago.
- Establezca o modifique los límites de gasto por proyecto.
- Consulta las tendencias de costos de cada proyecto.
- Consulta el AWS gasto total de todos los proyectos.
- Consulta y canjea los créditos promocionales que no son de la capa gratuita.
- Consulta los créditos restantes y las fechas de caducidad de todos los tipos de crédito.
- Consulta el historial crediticio completo, incluidos los créditos acumulados, aplicados y vencidos.
- Consulta cómo se aplican los créditos en todos los proyectos.
- Consulta el saldo pendiente.
- Ejecute pagos a AWS.
- Descarga facturas o consulta transacciones pasadas.
- Compruebe que AWS los cargos son correctos, incluidos los créditos aplicados.
- Reciba comunicaciones de facturación a nivel de cuenta de administración.
- Obtenga ayuda con los problemas de facturación a nivel de la organización.
- Solicita un aumento de cuota para las cuotas de cuenta y facturación.

Cómo acceden los miembros del equipo a tu AWS recursos

Nuestra nueva AWS experiencia crea un rol vinculado a un servicio para la organización que contiene todos tus proyectos que no puedes modificar. Este rol verifica periódicamente que los registros internos de los miembros de tu equipo estén sincronizados con los de los miembros reales de tu equipo.

El rol vinculado al servicio AWSServiceRoleForAccountAccessManager depende de los siguientes servicios para asumir el rol:

- `account-access.amazonaws.com`

La política de permisos de rol denominada `AccountAccessManagerServiceRolePolicy` permite al administrador de acceso a la cuenta completar las siguientes acciones en los recursos especificados:

- Acción:`organizations:ListAccounts`,`organizations:ListAWSServiceAccessForOrganizati`
  `organizations:DescribeAccount` activada `"arn:aws:organizations::*:account/o-*/*"`

Para obtener más información, consulte AWS Account Access Manager.

Invita a los miembros del equipo a colaborar en AWS Configuración

Para invitar a los miembros del equipo, envíales una invitación desde la página del equipo en la AWS configuración. Los miembros del equipo tienen 14 días para aceptar la invitación. Los miembros del equipo deben crear una ID de creador de AWS para acceder a tu proyecto. Pueden hacerlo usando Sign up for AWS (new).

Invita a los miembros del equipo a colaborar en AWS Configuración

1. Abre AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Equipo.
3. Selecciona Invitar a un nuevo miembro del equipo.
4. En Correo electrónico, introduce una dirección de correo electrónico o una lista de direcciones de correo electrónico. Separe las direcciones de correo electrónico con comas (,) o punto y coma (;).
5. Elige uno o más proyectos para compartirlos con los nuevos miembros de tu equipo.
6. Seleccione Send invitation (Enviar invitación).

Si los miembros de tu equipo no reciben la invitación, pídeles que revisen sus carpetas de correo no deseado y basura.

Invita a un miembro del equipo a un proyecto en AWS Configuración

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Puedes invitar a un miembro del equipo a acceder a un proyecto. Para obtener información sobre lo que los miembros del equipo pueden hacer en un proyecto, consulteInvita a los miembros del equipo a colaborar en AWS Configuración.

Para invitar a un miembro del equipo a un proyecto

1. Abre AWS Configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona el proyecto al que quieres acceder.
3. Para los miembros, selecciona Invitar a un nuevo miembro del equipo.
4. En Correo electrónico, introduce una dirección de correo electrónico o una lista de direcciones de correo electrónico. Separe las direcciones de correo electrónico con comas (,) o punto y coma (;).
5. Elige un proyecto para compartirlo con los nuevos miembros de tu equipo.
6. Seleccione Send invitation (Enviar invitación).

Si los miembros de tu equipo no reciben la invitación, pídeles que revisen sus carpetas de spam y papelera.

Eliminar a un miembro del equipo de un proyecto en AWS Configuración

> ⚠ Warning
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Puedes eliminar a un miembro del equipo de un proyecto en cualquier momento. Los miembros de tu equipo no pueden hacerlo solos. Cuando elimines a un miembro del equipo, este dejará de tener acceso a ese proyecto. Todos los recursos que haya creado el miembro de tu equipo permanecerán en tu proyecto y tú debes administrarlos.

Para eliminar un miembro del equipo de un proyecto

1. Abre AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, elige el proyecto al que deseas acceder.

3. En la pestaña Miembros, selecciona el miembro al que quieres eliminar del proyecto y, a continuación, elige Eliminar.
4. Confirma tu elección y elige Eliminar.

El miembro del equipo sigue siendo parte de tu equipo y puedes añadirlo a otros proyectos. Para eliminar por completo a un miembro del equipo de AWS la configuración, consultaEliminar a un miembro del equipo en AWS Configuración.

Eliminar a un miembro del equipo en AWS Configuración

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Puedes usar la página del equipo para eliminar a un miembro del equipo de todos los proyectos. Perderán automáticamente el acceso a cualquier proyecto. No se eliminarán los recursos que haya creado el miembro del equipo.

Para eliminar un miembro del equipo

1. Abre AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Equipo.
3. Selecciona la casilla del miembro del equipo que quieres eliminar.
4. Elija Eliminar .
5. Confirma tu elección y elige Eliminar.

Revocar una invitación a un miembro del equipo en AWS Configuración

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Puedes revocar una invitación pendiente. La invitación permanecerá en la AWS configuración durante 14 días. Al revocar una invitación pendiente, se desactivará el enlace de acceso que figura en el correo electrónico de invitación. No puedes revocar una invitación aceptada, sino eliminar al miembro del equipo. Para obtener más información, consulte Eliminar a un miembro del equipo en AWS Configuración.

Para revocar una invitación

1. Abre la AWS configuración en. https://settings.aws.com
2. En el panel de navegación principal, selecciona Equipo.
3. Selecciona la casilla del miembro del equipo que tiene una invitación pendiente.
4. Seleccione Revocar.
5. Confirma tu elección y elige Revocar invitación.

Reenviar una invitación a un miembro del equipo en AWS Configuración

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Puedes volver a enviar una invitación a un miembro del equipo si la invitación ha sido revocada, caducada o rechazada. Cuando vuelves a enviar una invitación, el miembro de tu equipo recibe un nuevo correo electrónico con una fecha de caducidad de 14 días a partir del momento en que reenvías la invitación.

Para reenviar una invitación

1. Abre la AWS configuración en. https://settings.aws.com
2. En el panel de navegación principal, selecciona Equipo.
3. Selecciona la casilla de verificación del miembro del equipo que tiene una invitación revocada, caducada o rechazada.
4. Selecciona Reenviar.

5. Confirma tu elección y elige Reenviar invitación.

Actualiza tu cuenta en AWS Configuración

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Cuando te registras en Sign up for AWS (new), tus cuentas pasarán a la capa gratuita. En la capa gratuita, recibes un crédito de registro de 100 USD y ganas hasta 100 USD en créditos adicionales. Cuando te quedes sin créditos o tengas una cuenta de más de 6 meses, tendrás que cambiarte a un plan de pago. También puedes cambiarte a un plan de pago en cualquier momento. Cuando cambias a un plan de pago, tienes acceso a los servicios que figuran en élServicios de AWS incluido en el plan de pago de nuestro nuevo AWS experiencia.

Consideraciones para actualizar tu cuenta

Cuando cambies a un plan de pago, ten en cuenta lo siguiente:

- No puedes actualizar proyectos individuales. Todos tus proyectos se actualizan cuando actualizas tu cuenta.
- Cuando actualices, tendrás acceso a los servicios de Always Free y a las ofertas de prueba a corto plazo.
- Puedes optar a otros descuentos y créditos promocionales.
- Debes pagar los cargos que superen el saldo del crédito.
- Puedes crear un límite de gasto para establecer lo máximo que pagarás al mes por un proyecto. Para obtener más información, consulte Crea un límite de gasto en AWS Configuración.
- No puedes designar ningún proyecto como compatible con la HIPAA o la SEC.
- Tu cuenta no se cierra cuando se agotan los créditos.
- Esto no te convierte en una mejora paraRegistrarse en AWS (avanzado). Ninguna de las funciones que solo son compatibles con las cuentas creadas con ellas Registrarse en AWS (avanzado) estará disponible cuando actualices tu cuenta. Sin embargo, puedes hacerlo Activar avanzado AWS Características de para tu cuenta.
- No puede revertir el proceso de actualización.

Actualice su cuenta en AWS Configuración

Para actualizar su cuenta

1. Abre AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Facturación.
3. Seleccione Actualizar.
4. Elija Comenzar.
5. Añade tu método de pago.

   Según tu ubicación, es posible que tengas que proporcionar algunos datos fiscales.
6. Selecciona Actualizar cuenta.
7. Elige Continuar para volver al edificio o elige Establecer límites de gasto para establecer un límite de gasto. Para obtener más información sobre los límites de gasto, consultaCrea un límite de gasto en AWS Configuración.
8. Selecciona Ir a la consola.

La actualización se ha completado.

Crea un límite de gasto en AWS Configuración

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

¿Qué es un límite de gasto?

Los límites de gasto permiten a AWS los desarrolladores confiar en que pueden operar dentro de un presupuesto predecible y controlado. Use un límite de gasto para establecer lo máximo que pagará al mes por un proyecto. Los límites de gasto se establecen por proyecto. Puede establecer límites de gasto en algunos de los proyectos y tener otros proyectos sin límites de gasto.

Si el uso que haces en un proyecto alcanza su límite, AWS detiene ese proyecto, lo que interrumpe sus recursos para que tus costes se mantengan dentro de los límites. Los límites de gasto están

diseñados para la experimentación, el aprendizaje y las cargas de trabajo aisladas. Se pueden usar en entornos de producción cuando sea aceptable hacer una breve pausa en los recursos en los casos en que las aplicaciones incurran en costes inesperados.

Los límites de gasto son visibles para cualquier persona que tenga acceso al proyecto, pero solo los propietarios de los proyectos pueden gestionarlos. Debes tener un plan de pago para crear un límite de gasto. Para obtener más información, consulte Actualiza tu cuenta en AWS Configuración.

Los límites de gasto son un tipo de AWS presupuesto.

Establece tu límite de gasto

Tu límite de gasto es el límite máximo de los costes antes de impuestos de tu proyecto, no una cuota. Cuando estableces un límite de gasto, el valor mínimo permitido es de 20$ o una estimación moderada del gasto probable, que sea mayor.

Por qué existe un mínimo: Alcanzar un límite de gasto es una experiencia disruptiva. El mínimo existe para que sea poco probable que las variaciones normales en el consumo provoquen que se alcance el límite de gasto.

Cómo se calcula la estimación conservadora: la estimación se basa en la actividad del mes hasta la fecha, pero no es una extrapolación lineal estricta. AWS analiza tus gastos hasta la fecha y los recursos de los que dispones actualmente. AWS también utiliza la actividad del mes anterior; si fue alta, se convierte en la mínima.

Si tiene muchos recursos disponibles: la estimación prudente de lo que probablemente gaste será alta. Si quieres establecer un límite de gasto más bajo, primero debes detener esos recursos.

Si vas a reactivar un proyecto en pausa: la estimación prudente del gasto probable es el gasto realizado hasta la fecha durante el mes, más el uso que no se haya cobrado.

> **Note**
>
> Los límites de gasto no incluyen los créditos y se aplican a los cargos antes de impuestos.

Notificaciones

Recibirás notificaciones cuando los costes reales alcancen el 50%, el 75% y el 90% de tu límite, o cuando estés a punto de alcanzar o superar tu límite de gasto en los próximos 10 días.

Personaliza la configuración de tus límites de gasto con controles de costes anticipados opcionales

Su límite de gasto evita que su factura supere el monto que usted estableció. Si tu consumo lo alcanza, AWS pausa tus recursos para protegerte. Estos controles opcionales actúan antes y con más suavidad, por lo que te mantienes muy por debajo del límite.

Detenga la creación de nuevos recursos

Unos 7 días antes de que alcances tu límite, dejarán de lanzarse nuevos recursos. Esto se logra mediante la aplicación de una política de control de servicios gestionada por AWS. La política de control del servicio depende del servicio. Para ver todas las políticas de control de servicios que podrían aplicarse a su proyecto, consultePolíticas de control de servicios para los límites de gasto.

Todos los recursos que ya están en ejecución permanecen en funcionamiento. En la mayoría de los casos, nada de lo que haya creado se verá afectado. Sin embargo, en algunos casos, esto podría provocar una experiencia perturbadora. Por ejemplo, si has activado el autoscaling y si se cumplen las condiciones para ejecutar esta acción, no se lanzarán nuevas instancias.

Pausa los recursos inactivos

Unos 5 días antes de que alcance el límite, los recursos inactivos se pausan. Las aplicaciones activas siguen ejecutándose. Los recursos inactivos se pausan según las recomendaciones de AWS Compute Optimizer. Para obtener más información, consulta Ver recomendaciones de inactividad.

También puede ver sus recomendaciones de recursos inactivos iniciando sesión en su proyecto y consultando las oportunidades de ahorro. Para obtener más información, consulte el Centro de optimización de costos. En este momento, como parte de tu experiencia con los límites de gastos, pausaremos automáticamente el EC2, el RDS y SageMaker los endpoints.

Por qué pausamos una instancia de EC2: pausamos las instancias de EC2 si el uso máximo de la CPU es inferior al 5% y su red I/O es inferior a 5 MB por día durante los últimos 14 días.

Si tiene un tipo de instancia G o P, hay un criterio de inactividad diferente. Los tipos de instancia G o P se pausarán si ocurre lo siguiente durante los últimos 14 días:

- La GPU no funciona activamente durante más del 99 % del periodo examinado
- El codificador de GPU no se usa durante el 99 % o más del tiempo de ejecución de la instancia

- El uso de memoria de la GPU a nivel de instancia es inferior al 5%
- La utilización máxima de la CPU es inferior al 5 %
- La utilización de la red es inferior al 5% MB/day

Por qué pausamos una base de datos de RDS: pausamos RDS para MySQL y RDS para PostgreSQL si la instancia de la base de datos no es una réplica de lectura y ha tenido lo siguiente en los últimos 14 días:

- No hay conexiones a bases de datos
- Bajo consumo de CPU
- Baja read/write actividad

Por qué pausamos un SageMaker punto final inactivo: pausamos SageMaker los puntos finales si el punto final no ha tenido ninguna invocación en los últimos 14 días.

Detenga los principales factores de costes

Aproximadamente 4 días antes de que alcance su límite, se suspende el costo más alto en el que incurren los recursos activos. Esta puede ser una experiencia perturbadora. En este momento, seleccionamos los recursos de estos cinco servicios: EC2, RDS, Lambda, Bedrock y. SageMaker Este control opcional puede evitar que incurra en costes si tiene una Lambda descontrolada o un repunte inesperado de Bedrock.

¿Qué ocurre si alcanzas tu límite

AWS hace una pausa en el proyecto y detiene todos los recursos. Sus datos se conservan.

Para reactivar tu proyecto, aumenta tu límite de gasto desde AWS Configuración. Tras la reactivación, es posible que algunos recursos deban reiniciarse manualmente.

> **Important**
>
> Si no realizas ninguna acción en un plazo de 90 días a partir de la pausa del proyecto, se eliminarán AWS permanentemente los datos del proyecto.

Otros aspectos importantes que debes tener en cuenta

- Si utilizas Amazon Route 53, solo puedes comprar un dominio cada 24 horas. Debe asegurarse de que los costos del dominio estén dentro de los límites de gasto; de lo contrario, la compra del dominio no se realizará. En esos casos, debes aumentar los límites de gasto antes de realizar una compra.
- Puedes aplicar límites de gasto a un máximo de 10 proyectos.

Crea un límite de gasto en AWS Configuración

Para crear un límite de gasto en AWS Configuración

1. Abre AWS Configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Facturación.
3. En Coste por proyecto, en Límite de gasto, selecciona Establecer límite para un proyecto.
4. Puedes elegir el límite de gasto recomendado o un límite personalizado.
5. Si eliges un límite personalizado, introduce el importe personalizado.
6. Elige Establecer límite de gasto.
7. Para personalizar tu límite de gasto con controles de costes anticipados, puedes seleccionar Detener el lanzamiento de nuevos recursos, Pausar los recursos inactivos o Pausar los principales factores de coste.
8. Selecciona Guardar los controles de costes anticipados.

El límite de gasto entrará en vigor inmediatamente.

Actualiza un límite de gasto en AWS Configuración

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

El propietario del proyecto puede actualizar el límite de gasto en los AWS ajustes en cualquier momento. Puedes aumentar o reducir tu límite de gasto o cambiar los controles de costes iniciales

opcionales. Si AWS ha bloqueado el lanzamiento de nuevos recursos o ha pausado recursos porque se acerca a su límite, puede aumentar su límite de gasto. Si tu proyecto se ha detenido porque has alcanzado el límite, aumenta el límite de gasto para reactivar el proyecto. Para obtener más información sobre cómo funcionan los límites de gasto, consulta. Crea un límite de gasto en AWS Configuración

Actualiza un límite de gasto en AWS Configuración

Para actualizar un límite de gasto

1. Abre AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Facturación.
3. En Coste por proyecto, en Límite de gasto, selecciona el icono del lápiz.
4. En Límite de gasto mensual (USD), introduce un nuevo límite de gasto.

   Te ofrecemos una recomendación basada en tu gasto actual.
5. Para modificar las protecciones que quieres que se apliquen a tu proyecto, selecciona Detener el lanzamiento de nuevos recursos, Detener los recursos inactivos o Detener los principales factores de coste.
6. Elija Guardar configuración.

Los cambios en el límite de gasto entrarán en vigor de inmediato.

Eliminar un límite de gasto en AWS Configuración

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

El propietario del proyecto puede eliminar un límite de gasto en los AWS ajustes en cualquier momento. Cuando elimines un límite de gastos, AWS dejará de supervisar tus costes ni realizará ningún control de costes inicial en tu proyecto. Para obtener más información sobre cómo funcionan los límites de gastos, consulteCrea un límite de gasto en AWS Configuración.

Eliminar un límite de gasto en AWS Configuración

Para eliminar un límite de gasto

1. Abre AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Facturación.
3. En Coste por proyecto, en Límite de gasto, selecciona el icono del lápiz.
4. Selecciona Eliminar límite.
5. Confirma tu elección y elige Eliminar.

Tu límite de gasto se eliminará de inmediato.

Nivel gratuito en nuestro nuevo AWS experiencia

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Puedes usar AWS Free Tier para explorar AWS los servicios sin compromisos de costos. Si es la primera vez que lo usa AWS, recibirá 100 USD en créditos después de crear una cuenta, independientemente del plan de cuenta que tenga. También puede obtener hasta 100 USD adicionales en créditos en todos sus proyectos al completar actividades. Para obtener más información sobre la obtención de créditos adicionales, consulte Obtenga créditos adicionales. Además, tiene acceso a más de 30 AWS servicios siempre gratuitos que ofrecen límites mensuales de uso gratuito.

El plan de cuenta gratuita es ideal para los clientes que deseen experimentar con AWS los servicios y crear pruebas de concepto sin coste alguno durante un máximo de seis meses. Durante ese periodo, no se generarán cargos hasta que actualice a un plan de cuenta de pago. Su plan de cuenta gratuita finalizará después de seis meses o cuando los créditos se hayan agotado por completo (lo que ocurra primero). Además, los planes de cuentas gratuitas no ofrecen acceso a determinados AWS servicios que consumirían rápidamente la totalidad del importe del crédito de la capa AWS gratuita ni las compras de hardware. Para ver una lista de los servicios que cumplen los requisitos del plan de cuenta gratuito, consulta AWS los servicios compatibles al suscribirse AWS (nuevos).

El plan de cuenta de pago es ideal para crear aplicaciones de producción que superen el importe del crédito inicial. Cuando el uso supera el saldo de créditos o cuando utilizas un servicio al que no se aplican créditos, pagas el precio estándar de pago por uso.

Todos los proyectos que tienes pertenecen al mismo tipo de plan. Si pasas al plan de cuenta de pago, todos tus proyectos tienen acceso a servicios adicionales y pagas los precios estándar de pago por uso para todos los proyectos. Para obtener más información, consulta Cómo actualizar tu cuenta en Configuración. AWS

Puedes usar la consola de administración de costos para hacer un seguimiento del uso de todos los AWS servicios que ofrecen la capa gratuita para tu proyecto.

Seguimiento del uso del nivel gratuito

> **Warning**
>
> En estos momentos estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

AWS Las alertas de uso de la capa gratuita te notifican automáticamente por correo electrónico cuando superas el 85 por ciento del límite de la capa gratuita para cada servicio. Para realizar un seguimiento adicional, puedes configurar tu uso hasta el 100% del límite de la capa gratuita estableciendo un presupuesto sin gastos. También puede filtrar el presupuesto para realizar un seguimiento de servicios específicos.

Puedes hacer un seguimiento del uso de la capa AWS gratuita de las siguientes maneras.

Utilización AWS Configuración

Puedes controlar la fecha de caducidad del plan de cuenta gratuita, el saldo de crédito y los días restantes en AWS Configuración. Para obtener más información, consulte Ver y canjear créditos en AWS Configuración. También recibirá alertas periódicas por correo electrónico sobre su saldo de crédito y cuando se acerca el final del periodo del plan de cuenta gratuita.

Si tienes un plan de pago, puedes controlar tu saldo de crédito y la fecha de caducidad en la página de créditos de AWS Configuración. Para obtener más información sobre la actualización a un plan de pago, consultaActualiza tu cuenta en AWS Configuración.

Uso de la consola de facturación y administración de costos

Puedes usar la consola de facturación y administración de costos para hacer un seguimiento del uso de la capa gratuita en cada proyecto. La consola de facturación y administración de costos muestra un resumen de tu uso mensual y de cualquier oferta de servicio que alcance los límites de uso o los supere. Para ver cada oferta de nivel gratuito en uso, puedes ver lo siguiente:

- El servicio
- El límite de uso de la capa AWS gratuita
- Tu uso actual
- Su uso previsto
- Tu consumo real en lo que va del mes (MTD)
- Su consumo previsto para el mes hasta la fecha (MTD)

El siguiente procedimiento muestra cómo usar la consola de facturación y administración de costos para ordenar el uso de la capa gratuita según el uso real del mes hasta la fecha.

Para ordenar el uso de la capa gratuita

1. Abra la consola de Administración de facturación y costos en https://console.aws.amazon.com/cost-management/.
2. Elige la capa gratuita.
3. Para ordenar por uso real del mes hasta la fecha, elige el% de uso real de MTD.

Obtenga créditos adicionales

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Si eres un AWS cliente nuevo, puedes ganar 100 USD adicionales en créditos, independientemente del plan de tu cuenta, al completar las actividades. Estas actividades le ayudan a conocer los AWS servicios. Puedes encontrar las actividades en el AWS widget Explorar del panel de inicio de la

AWS consola. Todas estas actividades generarán cargos de AWS servicio que se deducirán de los créditos de la capa AWS gratuita. Sin embargo, cuando completes cada actividad, recibirás 20 USD en créditos.

Actividades que debes completar

- Lance una instancia con Amazon EC2
- Utilice un modelo fundamental en el área de juegos de Amazon Bedrock
- Crea un presupuesto
- Cree una aplicación web con Lambda
- Cree una base de datos de Amazon RDS

Consulta tu información de facturación en AWS Configuración

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Puedes usar la AWS configuración para ver tu información de facturación. Si utilizas la capa gratuita, esta página te muestra cuántos días tienes de la capa gratuita y tus AWS créditos. También puedes ver el coste por proyecto. Si utilizas el plan de pago, puedes ver tu saldo, los cargos actuales y el costo por proyecto. Si utilizas un límite de gastos, puedes ver la información relacionada con ese límite. También puedes Gestiona tu método de pago en AWS Configuración yGestiona el registro de impuestos en AWS Configuración.

Cuando utilizas el plan gratuito, todo el uso está cubierto por tus créditos de la capa AWS gratuita. Debes pasarte al plan de pago si agotas los créditos del nivel AWS gratuito o transcurridos 184 días, lo que ocurra primero. Para obtener más información sobre la actualización a un plan de pago, consulteActualiza tu cuenta en AWS Configuración.

Para ver el costo por proyecto

1. Abre AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Facturación.

3. En Coste por proyecto, verás tus cargos mensuales y los cargos mensuales previstos. Verás todos los cargos de tus proyectos.
4. (Opcional) Para ver un desglose de los cargos de un proyecto en Inspeccionar costos, selecciona Ver. Se te redirigirá a la consola AWS de facturación y administración de costos.

Los datos de facturación y los datos del explorador de costos que aparecen en la consola de AWS facturación y administración de costos se actualizan al menos una vez al día. La cadencia cuando se actualizan puede variar. Si utilizas un límite de gastos, esto puede generar diferencias en los cargos estimados del mes hasta la fecha en la consola de AWS configuración y AWS gestión de costes.

Consulta tu historial de facturación en AWS Configuración

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Puedes ver tu historial de facturación en AWS Configuración. Tu historial de facturación solo está disponible si tienes un método de pago. Si utilizas la capa gratuita, no verás tu historial de facturación.

Puedes descargar las facturas de cada proveedor de servicios con el que hayas realizado transacciones durante el período de facturación. Esto incluye información como el tipo de cargo, la fecha de la factura y el total en USD. Si sus facturas se emiten en otra divisa, también se muestra el total en dicha divisa. Las facturas no se dividen en cada proyecto.

Para ver tu historial de facturación

1. Abre AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Facturación.
3. Junto a Saldo, selecciona Ver historial de facturación. Se te redirigirá al historial de facturación.
4. Para descargar una factura, selecciona un identificador de factura.

Gestiona tu método de pago en AWS Configuración

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Puedes gestionar tu método de pago en AWS Configuración. Tu método de pago se usa para pagar el uso de los AWS recursos en todos tus proyectos. Solo puedes administrar tu método de pago si proporcionaste información al crear tu cuenta o si cambiaste tu cuenta al plan de pago.

Para administrar tu método de pago

1. Abre AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Facturación.
3. En Saldo, verás tu información de pago. Elija Administrar.
4. En Método de pago, selecciona Actualizar.
5. Introduce tu nuevo método de pago y selecciona Guardar.

Realizar un pago en AWS Configuración

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Puedes pagar tu AWS factura en AWS Ajustes. AWS cobra automáticamente a tu método de pago predeterminado al principio de cada mes. Si dicho cargo no se procesa correctamente, use la consola para actualizar el método de pago y realizar un pago.

Antes de realizar un pago, asegúrate de que el método de pago al que quieres que se te cobre automáticamente en el futuro esté establecido como método de pago predeterminado. Si utiliza una tarjeta de crédito, confirme que no haya vencido.

Para realizar un pago

1. Abre AWS Configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Facturación.
3. Junto a Saldo, selecciona Ver historial de facturación. Se te redirigirá al historial de facturación.
4. En Acción, verás Pagar la factura de cualquier factura pendiente. Si no hay ninguna factura en la lista, no necesitas hacer nada.
5. Selecciona Pagar factura.
6. Confirma tu elección y elige Pagar.

Si tiene alguna pregunta sobre problemas con cargos en la cuenta bancaria o sobre el pago de un saldo pendiente, cree un caso en el Centro de soporte.

Cambia tu moneda preferida en AWS Configuración

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Puedes cambiar la moneda que prefieras en AWS Configuración. La moneda que prefieras solo se aplica a los proyectos de los que eres propietario. Algunos países de facturación restringen las monedas de pago. El emisor de tu tarjeta puede cobrar una comisión por las transiciones en otras monedas.

Para cambiar la moneda de visualización que prefieras

1. Abre AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Facturación.
3. En Saldo, verás tu información de pago. Elija Administrar. Si no ves el saldo, no puedes cambiar la moneda.
4. Selecciona Establecer moneda.
5. Para la moneda de pago predeterminada, selecciona la moneda de pago.

6. Seleccione Save.

Gestiona el registro de impuestos en AWS Configuración

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Gestionas tus números de registro fiscal y tus exenciones fiscales en AWS Configuración. Tu información fiscal solo se aplica a los proyectos de los que eres propietario.

Actualización y eliminación de números de identificación fiscal

Siga estos pasos para actualizar o eliminar uno o varios números de registro fiscal.

> **Note**
>
> Si un país no aparece en el menú desplegable de la página Configuración fiscal, AWS no recopila el registro fiscal de ese país en este momento.

Para actualizar números de identificación fiscal

1. Abre AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Facturación.
3. En Saldo, verás tu información de pago. Elija Administrar.
4. Selecciona Configuración de impuestos.
5. Modifica tu información de registro fiscal.
6. Seleccione Save.

Administrar sus exenciones fiscales de EE. UU.

Si tu estado cumple los requisitos, puedes gestionar tus exenciones fiscales de EE. UU. en la página Plan y facturación de la sección AWS Configuración. El equipo de soporte revisará los documentos

que subas para solicitar la exención en un plazo de 24 horas. Solo puedes gestionar tus exenciones fiscales si tu cuenta está registrada como empresa.

Si desea cargar o agregar su exención fiscal de EE. UU.

1. Abre la AWS configuración en. https://settings.aws.com
2. En el panel de navegación principal, selecciona Facturación.
3. En Saldo, verás tu información de pago. Elija Administrar.
4. Elija Manage tax exemption (Administrar la exención fiscal) y seleccione Add tax exemption (Agregar exención fiscal).
5. Especifique el tipo de exención y la jurisdicción.
6. Cargue documentos de certificado.
7. Revise la información y seleccione Submit (Enviar).

En un plazo de 24 horas, Support te notificará mediante un caso de soporte si necesitan información adicional o si alguno de tus documentos no es válido.

Una vez aprobada la exención, puede verla en la pestaña Exención fiscal con un periodo de validez Activo.

Se le notificará a través de un contacto de caso de soporte si se ha rechazado su exención.

Ver y canjear créditos en AWS Configuración

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Puedes ver y canjear los créditos disponibles en AWS Configuración. AWS los créditos se aplican automáticamente a las facturas para ayudar a cubrir los costos asociados a los servicios elegibles. Para obtener más información sobre los servicios elegibles, consulta Canjea tu crédito AWS promocional. Los créditos se aplican a todos los proyectos de tu propiedad hasta que se agoten o caduquen. No puedes seleccionar qué proyecto usa los créditos que canjeas, ya que se aplican a todos los proyectos que poseas.

Para ver tus créditos

1. Abre AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Facturación.
3. En el contenedor Cargos actuales, verás los créditos disponibles. Elige tus créditos.

   Se te redirigirá a una vista de los créditos activos y caducados, o a tus créditos y a los créditos inactivos de los últimos 6 meses, según el tipo de plan.
4. Para ver los AWS servicios que puedes usar con tus créditos, selecciona Ver lista de servicios.

Para canjear tus AWS Créditos promocionales

1. Abre AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Facturación.
3. En el contenedor Cargos actuales, verás los créditos disponibles. Elige tus créditos.

   Se te redirigirá a una vista de los créditos activos y caducados, o a tus créditos y a los créditos inactivos de los últimos 6 meses, según el tipo de plan.
4. Elige Canjear crédito para canjearlos.
5. Para el código promocional, introduce el código promocional tal como aparece. Al canjear el crédito, indicas que has leído y estás de acuerdo con los términos y condiciones de los créditos AWS promocionales.
6. Selecciona Canjear crédito.

Administre cuentas en India en AWS Configuración

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Si te registras AWS y eliges India como dirección de contacto y facturación, tu acuerdo de usuario se celebra con Amazon Web Services India Private Limited (AWS India), un AWS vendedor local en la India. AWS India gestiona la facturación y el total de la factura se indica en rupias indias (INR) en lugar de en dólares estadounidenses (USD).

Si su cuenta está en AWS India, siga los procedimientos de este tema para administrarla. En este tema se explica cómo abrir una cuenta en AWS India, editar la información sobre tu cuenta en AWS India, gestionar la verificación de clientes y añadir o editar tu número de cuenta permanente (PAN).

Temas

- Registrarse en AWS (nuevo) con AWS India
- Administre la información de verificación del cliente

Registrarse en AWS (nuevo) con AWS India

AWS India es un vendedor local AWS de India. Si tu dirección de contacto y facturación se encuentra en India, sigue el siguiente procedimiento para registrarte.

Para usar Regístrate en AWS (nuevo) con AWS India

1. Ve a aws.amazon.com y selecciona Crear cuenta.
2. En el banner que explica las diferencias entre Registrarse en AWS (nuevo) y Registrarse en AWS (avanzado), selecciona Registrarse en. AWS
3. Elige un inicio de sesión como Google GitHub, Apple o Amazon.
4. Se te dirigirá al inicio de sesión de tu proveedor. Después de iniciar sesión, se te redirigirá para que te AWS registres.
5. Introduce tu nombre y selecciona Continuar.

   Este nombre se compartirá con los miembros del equipo cuando les des acceso a tus proyectos.
6. Verifica el correo electrónico asociado a tu inicio de sesión introduciendo un código de verificación. Cuando hayas verificado tu correo electrónico, selecciona Continuar.
7. Introduce una contraseña segura para tu cuenta y selecciona Continuar.

   AWS requiere que la contraseña cumpla las siguientes condiciones:

   - Debe tener 8 caracteres como mínimo y 128 como máximo.
   - Debe incluir un mínimo de tres de los siguientes tipos de caracteres: mayúsculas, minúsculas, números y! @ # $% ^ portal de administración * () <> [] {} | _+-= símbolos.
   - No debe ser idéntico a su Cuenta de AWS nombre o dirección de correo electrónico.
8. Introduce tus datos de contacto y selecciona Continuar.

Si su dirección de contacto o facturación se encuentra en la India, de conformidad con las normas del Equipo de Respuesta a Emergencias Informáticas de la India (CERT-In), AWS debe recopilar y validar su información de identidad antes de concederle acceso a AWS los servicios.

El nombre de su información de contacto o de facturación debe coincidir con el nombre que aparece en el documento que piensa usar para la verificación del cliente. Por ejemplo, si planea verificar una cuenta empresarial mediante un certificado de constitución, debe proporcionar el nombre comercial que aparece en el documento. Para obtener una lista de los tipos de documentos aceptados, consulte the section called “Documentos de la India aceptados para la verificación del cliente”.

9. Elija el propósito principal del registro de su cuenta.
10. Elija el tipo de propiedad que mejor representa al propietario de la cuenta. Si elige una empresa, organización o asociación como el tipo de propiedad, ingrese el nombre del contacto administrativo clave. El contacto administrativo clave puede ser un director, un jefe de operaciones o una persona a cargo de las operaciones de su empresa.
11. En función del tipo de propiedad que haya seleccionado, elija un documento aceptado de la India para utilizarlo en la verificación e ingrese su información de documento.

> **Note**
>
> Si tiene una cuenta personal y planea usar un permiso de conducir no emitido por la Unión de la India, le recomendamos que utilice un tipo de documento personal diferente para la verificación.

12. Seleccione el nombre que desea utilizar para la verificación del cliente.

    Los nombres de su información de contacto y facturación aparecerán para que los seleccione si están asociados a una dirección de la India. Asegúrese de que el nombre elegido coincide con el nombre del tipo de documento que piensa usar para la verificación del cliente. Si necesita modificar el nombre asociado a su dirección de contacto o facturación, puede hacerlo una vez completado el registro de la cuenta.
13. Autorice el envío de su información a efectos de verificación y, a continuación, seleccione Continuar.

    Recibirá una notificación por correo electrónico sobre el resultado de la verificación del cliente después de completar el inicio de sesión de la cuenta. También puedes comprobar el estado

en la página de perfil en Mis AWS ajustes. Para acceder a los servicios de AWS , debe pasar la verificación del cliente.

14. AWS aprovisionará tu primer proyecto.

Para acceder a AWS la configuración, selecciona Administrar proyectos en Consola de administración de AWS. En AWS Configuración, puedes invitar a miembros del equipo, crear nuevos proyectos y modificar la facturación y otros ajustes.

Administre la información de verificación del cliente

De conformidad con las normas del Equipo de Respuesta a Emergencias Informáticas de la India (CERT-In), AWS es obligatorio recopilar y validar su información de identidad antes de concederle un acceso nuevo o continuo a AWS los servicios. Para verificar su identidad, deberá utilizar el nombre de la dirección de contacto o facturación de la India que haya facilitado. Durante la verificación, AWS comprobará si el número de documento es válido y si el nombre que has proporcionado coincide con el nombre asociado al documento que utilizas para la verificación del cliente. El nombre de su información de contacto o de facturación debe coincidir con el nombre que aparece en el documento.

Para actualizar tu nombre de facturación, dirección y demás información de contacto, consultaUso AWS Configuración. Si editas cualquier información que utilizaste anteriormente para la verificación de clientes, como el nombre o la India-based dirección de tu información de facturación o de contacto, es posible que tengas que actualizar y volver a enviar tu información de verificación de cliente.

Compruebe el estado de verificación del cliente

Puedes ver el estado de verificación de tu cliente en cualquier momento en la página Administrar perfil. Si el estado de verificación indica Verificación obligatoria o Verificación errónea, cree o actualice la información de verificación del cliente y envíela de nuevo para su posterior verificación.

Cree la información de verificación del cliente

Para completar la verificación como cliente, tendrá que proporcionar la información de un documento aceptado en la India. Para obtener una lista de los tipos de documentos aceptados, consulte the section called “Documentos de la India aceptados para la verificación del cliente”.

1. Abre AWS Configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Administrar perfil.

3. Para la verificación del cliente, selecciona Crear verificación del cliente.
4. Elija el nombre que coincide exacto con el nombre del documento que piensa usar para la verificación del cliente. Por ejemplo, si planea verificar una cuenta empresarial mediante un certificado de constitución, debe proporcionar el nombre comercial que aparece en el documento.
5. Proporcione el resto de la información solicitada en la página. Según el tipo de documento que elija, es posible que tenga que cargar una copia tanto del anverso como del reverso del documento. Si sube un archivo de imagen, asegúrese de que toda la información del documento esté visible y sea legible.
6. Seleccione Enviar.

   Se le notificará el resultado de la verificación del cliente y cualquier paso siguiente por correo electrónico o en el AWS Health Dashboard.

Edite la información de verificación del cliente

Puede editar la información de verificación de sus clientes, como el propósito principal del registro de la cuenta, el tipo de organización y el nombre, el tipo de documento, la carga del documento o la información del documento que desea usar para la verificación.

Si edita el nombre o tipo de documento para realizar la verificación del cliente, o actualiza la información del documento y guarda los cambios, se volverá a verificar su identidad.

1. Abre AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Administrar perfil.
3. Para la verificación del cliente, selecciona Verificación del cliente.
4. Elija Editar y, a continuación, actualice la información que desea cambiar.

   A medida que actualice la información, tenga en cuenta las siguientes instrucciones:

   - Si elige un nombre diferente, el nombre debe coincidir exacto con el nombre del documento que piensa usar para la verificación del cliente. Por ejemplo, si planea verificar una cuenta empresarial mediante un certificado de constitución, debe proporcionar el nombre comercial que aparece en el documento.
   - Si elige un tipo de documento diferente, tendrá que cargar una copia del anverso y el reverso (si corresponde) del documento. Toda la información de la carga del documento debe ser visible y legible.

- Si tiene una cuenta personal y planea usar un permiso de conducir no emitido por la Unión de la India, le recomendamos que utilice un tipo de documento personal diferente para la verificación.
- Para obtener una lista de los tipos de documentos aceptados, consulte the section called "Documentos de la India aceptados para la verificación del cliente".

5. Seleccione Enviar.

   Si es necesario volver a verificar su identidad debido al tipo de cambios que ha guardado, se le notificará el resultado de la verificación por parte del cliente y los pasos a seguir por correo electrónico. También puede ver los resultados volviendo a la página de verificación del cliente o al AWS Health Dashboard.

Documentos de la India aceptados para la verificación del cliente

Para la verificación del cliente, se aceptan los siguientes tipos de documentos expedidos por el gobierno de la India.

> **Note**
>
> Los enlaces compartidos a continuación pueden sufrir modificaciones a discreción del Gobierno.

- Tarjeta PAN: disponible en formato digital y físico, la tarjeta de número de cuenta permanente (PAN) contiene un identificador alfanumérico único expedido por el Departamento de Impuestos sobre la Renta de la India a personas físicas, empresas y entidades. Un PAN consta de diez caracteres, incluidos letras y números, con el formato **`AAAAA1111A`**. Para usar este documento como verificación, también debe proporcionar la fecha de nacimiento (persona física) o la fecha de constitución (empresa) que aparece en el documento PAN y cargar la parte frontal de la tarjeta. Para comprobar la validez de su PAN, consulte el sitio web oficial del Departamento de Impuestos sobre la Renta.
- Identificación de elector Card/EPIC: la tarjeta de identificación de votante, también conocida como tarjeta de identidad con fotografía del elector (EPIC), contiene un número de identificación único emitido por la Comisión Electoral de la India a los votantes elegibles en la India. El ID/EPIC número de elector consta de diez caracteres, que incluyen letras y números. Para comprobar la validez de su identificación de votante, consulte el sitio web oficial de la Comisión Electoral de la

India. Para usar este documento para la verificación, debe cargar tanto el anverso como el reverso de la tarjeta.

- Licencia de conducir: si su licencia de conducir no ha sido emitida por la Unión de la India, le recomendamos que utilice un tipo de documento diferente para la verificación. Un número de licencia de conducir consta de entre 12 y 16 caracteres, incluidos letras, números, espacios y guiones. Para usar este documento para la verificación, debe proporcionar la fecha de nacimiento y cargar tanto el anverso como el reverso de la tarjeta. Para comprobar la validez de su licencia de conducir, consulte el sitio web Parivahan Sewa del Ministerio de Transporte y Vialidad.
- Certificado de constitución: un certificado de constitución es un documento emitido por el Ministerio de Asuntos Corporativos (MCA) que fecha el registro de una empresa como entidad legal. El certificado se utiliza para identificar y localizar de manera exclusiva a las empresas registradas en la India. Cada certificado contiene un número de identificación corporativa (CIN), que es un identificador alfanumérico único que consta de 21 caracteres, incluidos letras y números. Para utilizar este documento para la verificación, debe cargar el documento del certificado de constitución. Puede ir al portal del Ministerio de Asuntos Corporativos para comprobar la validez de su CIN.

Se aceptan distintos tipos de documentos de la India para la apertura de cuentas personales y empresariales:

- Para cuentas personales: tarjeta PAN card/EPIC, identificación de votante y licencia de conducir.
- Para cuentas comerciales: tarjeta PAN y certificado de constitución.

Configura tu facturación en India en AWS Configuración

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Si te registras AWS y eliges la India como dirección de contacto y facturación, tu acuerdo de usuario se suscribe a Amazon Web Services India Private Limited (AWS India), un AWS vendedor local de la India. AWS India gestiona tu facturación y el total de la factura aparece en rupias en lugar de en dólares. Toda la información tributaria solo la puede crear o modificar el propietario del proyecto.

Para obtener información fiscal o de facturación adicional, puedes usar la AWS Billing consola para cada proyecto.

Usa la sección Plan y facturación de la página Administrar perfil de AWS Configuración para realizar las siguientes tareas:

- Agregar o editar un número de cuenta permanente
- Editar varios números de cuenta permanente
- Editar varios números de impuestos de bienes y servicios
- Ver una factura fiscal

Agregar o editar un número de cuenta permanente

Puede agregar su Número de cuenta permanente (PAN) a su cuenta y editarlo.

Para añadir o editar un PAN

1. Abre AWS Configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Administrar perfil y, a continuación, elige Plan y facturación.
3. En la barra de navegación Tax Settings, elija Edit.
4. En Permanent Account Number (PAN), escriba su PAN y después elija Update.

Editar varios números de cuenta permanente

Puede editar varios números de cuenta permanente (PAN) de su cuenta.

Para editar varios números PAN

1. Abre AWS Configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Administrar perfil y, a continuación, elige Plan y facturación.
3. En Manage Tax Registration Numbers (Administrar los números de identificación fiscal), seleccione los números PAN que desea editar.
4. En Manage Tax Registration (Administrar registro fiscal), elija Edit (Editar).
5. Actualice los campos que desee cambiar y elija Update (Actualizar).

Editar varios números de impuestos de bienes y servicios

Puede editar varios números de impuestos de bienes y servicios (GST) de su cuenta.

Para editar varios números GST

1. Abre AWS Configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Administrar perfil y, a continuación, elige Plan y facturación.
3. En Manage Tax Registration Numbers (Administrar los números de identificación fiscal), seleccione los números GST que desea editar o elija Edit all (Editar todo).
4. En Manage Tax Registration (Administrar registro fiscal), elija Edit (Editar).
5. Actualice los campos que desee cambiar y elija Update (Actualizar).

Ver una factura fiscal

Puedes ver tus facturas de impuestos en AWS Configuración.

Para ver una factura fiscal

1. Abre AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Administrar perfil y, a continuación, elige Plan y facturación.
3. Desplácese hacia abajo y elija la pestaña Facturas.
4. En la sección Facturas fiscales, elige el enlace a la factura que se menciona en la ID del documento.

> **Note**
>
> La sección Facturas fiscales solo se muestran si hay facturas fiscales disponibles.

Cambiar el nombre del vendedor registrado a o desde AWS India

Puedes cambiar tu Cuenta de AWS vendedor registrado (SOR) a otro SOR actualizando tu información fiscal o de facturación. Esto no se aplica si tu cuenta de AWS la India funciona con el

modelo anterior, en el que la funcionalidad no está disponible. Al editar el país o región en los datos fiscales o de facturación de su , el SOR cambiará automáticamente si el proveedor de servicios de la nueva ubicación es diferente de su ubicación actual.

Si cambias tu cuenta desde o hacia AWS la India, no necesitas actualizar tu método de pago predeterminado si está configurado como facturación o transferencia bancaria. Si su método de pago predeterminado es una tarjeta de crédito o débito, tendrá que volver a confirmar los detalles de la tarjeta de pago predeterminada. Esto tiene como finalidad garantizar que el método de pago se almacene por separado de las transacciones fuera de AWS India. Para obtener más información, consulta Cómo ver las tarjetas de crédito o débito aptas para las facturas de AWS la India.

> **Note**
>
> Si tienes una cuenta en AWS la India con una tarjeta de crédito o débito como método de pago predeterminado y tienes un mandato electrónico configurado para los pagos automáticos, debes desactivar el mandato electrónico antes de poder editar tus preferencias de pago predeterminadas.

Para cambiar el SOR de su cuenta, puede editar esta información mediante las siguientes opciones:

Para cambiar el SOR mediante la información fiscal y de facturación

1. Abre AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Administrar perfil y, a continuación, elige Plan y facturación.
3. En la sección Default payment preferences (Preferencias de pago predeterminadas), elija Edit (Editar).
4. Ingrese la nueva dirección de facturación.
5. En la sección Divisa de pago, elija una divisa predeterminada de la lista de divisas aceptadas del nuevo SOR.
6. (Si su método de pago predeterminado es una tarjeta de crédito o débito) En la sección Confirmar método de pago, vuelva a ingresar los detalles de su tarjeta de pago predeterminada para confirmar su uso con el nuevo proveedor de servicios.

   Para cambiar las tarjetas predeterminadas con el nuevo SOR, agregue su tarjeta más adelante y cambie la configuración del método de pago predeterminado.

7. Seleccione Save changes (Guardar cambios).

   Transcurridos unos minutos, los cambios, con el SOR actualizado, aparecerán en la página Preferencias de pago.

Para cambiar el SOR mediante la información de facturación e impuestos

Para trasladar su cuenta a un SOR diferente, debe actualizar el número de registro fiscal (TRN) asociado a la cuenta e ingresar un TRN nuevo y válido. También puede eliminar el TRN asociado a la cuenta. El nuevo SOR de su cuenta se resuelve automáticamente según el país de su nueva dirección fiscal y de su dirección de facturación actual, en orden de disponibilidad y prioridad. Cuando el SOR de tu cuenta cambie, recibirás una notificación de que tu cuenta se va a mudar a la AWS India o a salir de ella.

1. Abre AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Administrar perfil y, a continuación, elige Plan y facturación.
3. Seleccione su cuenta y elija Administrar registro fiscal y, a continuación, elija Editar, Editar todo o Eliminar TRN.
4. (Si tu método de pago predeterminado es una tarjeta de crédito o débito) En el panel de navegación principal, selecciona Administrar perfil y, a continuación, elige Plan y facturación.
5. Seleccione Agregar método de pago para volver a ingresar los detalles de su tarjeta de pago predeterminada o agregar una nueva tarjeta de pago.
6. En cuanto la tarjeta esté guardada, seleccione Establecer como predeterminada.

   La sección de Preferencias de pago predeterminadas avisa de que su método de pago predeterminado anterior no califica para su uso en el nuevo SOR. Actualice la página después de agregar su tarjeta de pago para que desaparezca esta alerta.

Acceso AWS Soporte

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Al suscribirse a nuestra nueva AWS experiencia, hay dos lugares en los que puede trabajar con AWS Support.

Puede acceder a Basic Support o Business Support+. De forma predeterminada, está inscrito en Basic Support. Puede iniciar una versión de prueba de Business Support+ para usarla de forma gratuita durante un máximo de seis meses.

Soporte para proyectos

Si tienes problemas con tu proyecto, la gestión de tu equipo o problemas relacionados con la facturación, puedes acceder a Basic Support o Business Support+ en AWS Configuración. Puedes solicitar proyectos adicionales para tu organización o solicitar aumentos de cuota relacionados con la facturación.

Crear un caso de soporte

1. Abre AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Support.
3. Para obtener soporte en proyectos, selecciona Crear caso.
4. En Asunto, introduce el asunto de tu caso de soporte.
5. En Descripción, describe tu problema. Si puedes, describe los pasos para reproducir el problema.
6. Seleccione Crear caso.

Después de crear un caso de soporte, puede ver la información del mismo para seguir trabajando con el soporte.

Para ver la información de tu caso

1. Abre AWS Configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Support.
3. Elija su caso de soporte. En esta vista, puede ver todas las comunicaciones sobre su caso.
4. Para enviar una respuesta al servicio de asistencia, en Responder, introduce tu respuesta y, a continuación, selecciona Enviar respuesta.

Cuando se resuelva tu caso, puedes resolverlo para eliminarlo de la AWS Configuración.

Para resolver tu caso

1. Abre AWS Configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Support.
3. Elija Resolver caso.

No podrás acceder a los detalles del caso una vez que se haya resuelto.

Soporte técnico

Si tiene problemas con sus AWS recursos, necesita asistencia técnica. Para acceder al soporte técnico, abre un caso en el AWS Support Center del proyecto que tiene el problema.

Support si todos sus proyectos y organización están cerrados

Si todos sus proyectos y su organización están cerrados, póngase en contacto con el servicio de asistencia rellenando el formulario Support Feedback.

En la sección Solicitud de información, en Cómo podemos ayudarte, indica que estás utilizando nuestra nueva AWS experiencia y que todos tus proyectos están cerrados.

Inicie una prueba de Business Support+

Puedes obtener Business Support+ gratis durante un máximo de seis meses. Business Support + se ofrece sin coste alguno hasta el 31 de octubre de 2026. A partir del 1 de noviembre de 2026, comenzarán los precios estándar y recibirás 174 USD en créditos de Business Support+ para cubrir hasta seis meses de 29 USD al mes. Permanecerás suscrito cuando finalice el período gratuito y comiencen los créditos, y te AWS notificará cuando tu saldo de crédito se agote antes de que comience la facturación del precio completo.

El cargo de Business Support+ es de $ 29/month o un porcentaje de tu AWS gasto, lo que sea mayor. Para obtener más información, consulta los detalles de precios. Tu plan se renueva mensualmente hasta que lo canceles.

Para iniciar la versión de prueba de Business Support+

1. Abre AWS Configuración en. https://settings.aws.com
2. En el panel de navegación principal, selecciona Support.

3. Selecciona Iniciar prueba. Esto afectará a todos los proyectos de su organización.
4. Revisa los términos, selecciona la casilla del acuerdo y, a continuación, selecciona Iniciar la prueba.

Puedes cancelar en cualquier momento sin compromiso ni penalización. Al cancelar, el acceso a Business Support+ finaliza inmediatamente y se pierden los créditos no utilizados. Puedes volver a inscribirte al precio estándar en cualquier momento, pero la oferta promocional de Business Support+ no se puede restablecer una vez cancelada.

Para cancelar Business Support+

1. Abre AWS Configuración en. https://settings.aws.com
2. En el panel de navegación principal, selecciona Support.
3. Selecciona Cancelar plan.
4. Seleccione la casilla de verificación para confirmar que al cancelar Business Support+ volverá a Basic Support inmediatamente, que perderá el acceso a las ventajas enumeradas y que sus 174$ en créditos se eliminarán y no podrán restablecerse.
5. Selecciona Cancelar plan para volver a Basic Support.

Supervise su proyecto mediante AWS CloudTrail

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Supervise su proyecto mediante AWS CloudTrail

Su proyecto está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un miembro del equipo o AWS servicio. CloudTrail captura todas las llamadas a la API de tu proyecto como eventos. Las llamadas capturadas incluyen las llamadas de la consola y las operaciones de la API para todos los AWS servicios compatibles. Con la información recopilada por CloudTrail, puedes determinar la solicitud que se realizó a tu proyecto, la persona que la hizo, cuándo se hizo y detalles adicionales.

Se usa CloudTrail para ver quién modificó el proyecto

Este tutorial es para usuarios que se sientan cómodos con el AWS CLI. Si compartes tu proyecto con varios miembros del equipo, puedes usarlo CloudTrail para ver quién modificó los recursos de tu proyecto. El `onBehalfOf` parámetro registra todas las acciones realizadas por ti o por los miembros del equipo cuando utilizan la AWS configuración o Consola de administración de AWS para acceder a tu proyecto. Este parámetro muestra un ID de usuario y un ID de almacén de identidades. Juntos, estos valores definen un ID de constructor al que has invitado a acceder a tu proyecto.

Para encontrar el `onBehalfOf` parámetro y conectarlo con un miembro del equipo, necesitarás acceder a AWS CLI y al Consola de administración de AWS. Si no lo tienes AWS CLI configurado, puedes usarlo AWS CloudShell para acceder a un shell preautenticado y basado en el navegador que puedes iniciar directamente desde allí y ejecutar comandos. Consola de administración de AWS AWS CLI

Paso 1. Para buscar un AWS CloudTrail Evento

1. Inicie sesión en Consola de administración de AWS y abra la CloudTrail consola en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, elija Event history (Historial de eventos). Verá una lista filtrada de eventos, con los últimos eventos en primer lugar. Elija un evento.
3. En el registro del evento, verás el siguiente contenido:

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

   Esta es la identidad que define al miembro del equipo que creó el CloudTrail evento.

Paso 2. Para conectar el BehalfOf parámetro on a un miembro del equipo

Para conectar el `onBehalfOf` parámetro a un miembro del equipo mediante AWS CLI:

Para utilizar el AWS CLI en tu terminal

1. Ejecute el siguiente comando para iniciar sesión en AWS CLI. Puedes encontrar tu región usandoRegiones de AWS para tus proyectos.

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

2. Ejecute el siguiente comando para obtener el ID de su almacén de identidades. El CloudTrail evento muestra el ARN del almacén de identidades, pero no indica el ID del almacén de identidades. Siempre Región de AWS `us-east-1` se utiliza para buscar el ID de su almacén de identidades.

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

El resultado será similar al siguiente:

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

Quieres copiar el ID del almacén de identidades. En este caso, el ID del almacén de identidades es`d-000000`.

3. Ejecute el siguiente comando para describir al miembro del equipo que corresponde al `onBehalfOf` parámetro.

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

El resultado será similar al siguiente:


```
{
    "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"
}
```


En este resultado se incluyen el nombre para mostrar y los correos electrónicos del miembro del equipo.

Para conectar el `onBehalfOf` parámetro a un miembro del equipo mediante AWS CloudShell, inicia sesión en Consola de administración de AWS y accede CloudShell. Para obtener más información, consulta Cómo empezar con AWS CloudShell. Dispondrá automáticamente de los permisos de acceso CloudShell de IAM correctos.

Cerrar un proyecto en AWS Configuración

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Si ya no necesitas tu proyecto, puedes cerrarlo. Tras cerrar el proyecto, puedes volver a abrirlo en un plazo de 90 días a partir del día en que lo cerraste. El tiempo transcurrido entre el día en que cerraste el proyecto y el momento en que lo cierra AWS permanentemente es el período posterior al cierre.

Lo que necesita saber antes de cerrar su proyecto

Antes de cerrar el proyecto, ten en cuenta lo siguiente:

- No puedes cerrar tu proyecto si está en pausa debido a que se ha superado un límite de gasto. Tienes que desactivar los límites de gasto y, a continuación, cerrar el proyecto. Para obtener más información, consulte Actualiza un límite de gasto en AWS Configuración.
- Todos los miembros del equipo perderán automáticamente el acceso a este proyecto y a todos los recursos que contiene.
- El cierre de su proyecto servirá como aviso de rescisión del acuerdo con el AWS cliente para este proyecto.
- No necesitas eliminar los recursos de tu proyecto antes de cerrarlo. Sin embargo, le recomendamos que haga una copia de seguridad de los recursos o datos que desee conservar. Para obtener instrucciones sobre cómo hacer una copia de seguridad de un recurso en particular, consulta la AWS documentación correspondiente a ese servicio.
- Puedes volver a abrir tu proyecto durante el período posterior al cierre. Los cargos por los servicios que permanecieron en tu proyecto se reanudarán si lo vuelves a abrir. También eres responsable de las facturas impagas.
- Sigues siendo responsable de todas las comisiones y cargos pendientes por los servicios consumidos antes del cierre del proyecto. Recibirás una AWS factura al mes siguiente de cerrar tu proyecto. Por ejemplo, si cerró su cuenta el 15 de enero, recibirá una factura a principios de febrero por el uso realizado entre el 1 y el 15 de enero.

- Una vez cerrado un proyecto, AWS te enviaremos correos electrónicos diarios durante un máximo de cinco días antes de que suspendamos el dominio. Una vez suspendido el dominio, y en función del registrador del dominio, eliminaremos el dominio en un plazo de 30 días o cederemos el dominio a su registrador. Para obtener más información, consulte Mi dominio Cuenta de AWS está cerrado o cerrado permanentemente y Mi dominio está registrado en Route 53. Esta información está escrita para los proyectos Cuentas de AWS, pero es precisa.
- AWS CloudTrail es un servicio de seguridad fundamental. Esto significa que las rutas creadas por los usuarios pueden seguir existiendo y generar eventos incluso después de cerrar un proyecto, a menos que un usuario elimine explícitamente las rutas de su proyecto antes de cerrarlo. Para obtener más información sobre cómo solicitar la eliminación de rutas después de que se Cuenta de AWS haya cerrado una, consulta la sección sobre el Cuenta de AWS cierre y las rutas en la Guía del CloudTrail usuario. Esta información está escrita para los proyectos Cuentas de AWS, pero la información es precisa.

Para cerrar un proyecto

Para cerrar un proyecto

1. Abra AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, elige el proyecto al que deseas acceder.
3. En Cerrar proyecto, elija Cerrar proyecto.
4. Confirme su elección y elija Cerrar proyecto.

La página del proyecto seguirá mostrando tu proyecto durante 90 días hasta que se elimine de forma permanente.

Post-closure periodo

El período posterior al cierre se refiere al tiempo que transcurre entre el día en que se cierra la cuenta y el momento en que se cierra el proyecto de AWS forma permanente. El periodo posterior al cierre es de 90 días. Durante el período posterior al cierre, solo podrás acceder a tu contenido y AWS servicios si vuelves a abrir tu proyecto. Tras el período posterior al cierre, cierra tu proyecto de AWS forma permanente y ya no puedes volver a abrirlo. AWS también eliminará el contenido y los recursos de tu cuenta (excepto las CloudTrail rutas). Una vez que un proyecto se ha cerrado de forma permanente, su ID de proyecto no se puede volver a utilizar.

Reabrir tu proyecto

Tu proyecto se cerrará permanentemente en 90 días, después de los cuales no podrás volver a abrirlo y AWS eliminarás el contenido que quede en él. Para reabrir tu proyecto antes de que se cierre definitivamente, (1) debes ponerte en contacto con nosotros lo antes Soporte posible y (2) debemos recibir el pago completo de cualquier saldo pendiente, incluida la información requerida tal y como se especifica en la factura, en un plazo de 60 días a partir de la fecha de cierre de la cuenta.

> **Note**
>
> Los cargos por los servicios que permanecieron en tu proyecto se reanudarán si lo vuelves a abrir.

Activar avanzado AWS Características de

> **Warning**
>
> Actualmente lanzamos nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Al activar las funciones avanzadas, asumes el control total de la AWS organización, la cuenta de gestión y la cuenta de administrador delegado que se utilizan para gestionar los proyectos que has creado y los miembros del equipo a los que has invitado. Administrará directamente la seguridad, la gobernanza y la composición del equipo de su AWS entorno. Tiene acceso a AWS servicios adicionales, capacidades multirregionales y controles administrativos y de facturación mejorados.

Debe actualizar su cuenta antes de activar las funciones avanzadas. Para obtener más información, consulte Actualiza tu cuenta en AWS Configuración.

¿Qué ocurre cuando activas las funciones avanzadas

Al activar las funciones avanzadas, los siguientes cambios se aplicarán inmediatamente a su cuenta de administración y a la AWS organización que contiene sus proyectos:

- Ahora eres el administrador de la AWS organización que contiene tus proyectos.

- Has establecido una dirección de correo electrónico raíz para tu cuenta de administración. También tendrás que configurar la contraseña del usuario raíz. Para obtener más información, consulte Establezca una contraseña de usuario root para su cuenta de administración.
- Administra sus proyectos como cuentas de miembros en su organización. Como administrador de esta organización, puede crear cuentas de miembros en la organización. Tu ID de AWS constructor sigue siendo el propietario de tus cuentas de proyecto. Para obtener más información, consulte Proyecte las cuentas después de activar las funciones avanzadas.
- Para asignar un rol de administrador a las cuentas de los miembros que invite a unirse a su organización, debe crear una OrganizationAccountAccessRole. Para obtener más información, consulte Crear la cuenta OrganizationAccountAccessRole en un miembro invitado.
- Los miembros de tu equipo se denominan identidades de personal y pueden seguir accediendo a tus AWS cuentas. También puede optar por personalizar la fuente de identidad de sus empleados mediante el Centro de identidad de IAM. Puede seguir utilizando AWS Builder ID como fuente de identidad o puede cambiarla por una fuente de identidad externa. Si cambias tu fuente de identidad de AWS Builder ID a otra fuente de identidad, es irreversible. No podrás volver a habilitar AWS Builder ID como fuente de identidad en el futuro. Para obtener más información, consulte Cambiar la fuente de identidad de AWS ID de creador.
- Puede controlar el AWS acceso de los usuarios y grupos a su instancia de organización del IAM Identity Center mediante el administrador de acceso a la cuenta. Puede utilizar esta función para modificar el acceso de los usuarios y, al mismo tiempo, permitir que sus usuarios inicien sesión `aws login` para recibir sus credenciales de sesión de rol de IAM desde el navegador. Para obtener más información, consulte el Administrador de acceso a la AWS cuenta.
- AWS crea una cuenta de miembro denominada Identity Delegated Admin en su organización con una función de administrador delegado. Esta función se utiliza para realizar la mayoría de las tareas administrativas en el Centro de Identidad de IAM y en el administrador de acceso a las cuentas. La función de administrador delegado debe utilizarse en EE. UU. Este (Norte de Virginia). Para obtener más información, consulte Administración delegada.

  Su ID de AWS creador es el propietario de la cuenta de administrador delegado de Identity, al igual que sus cuentas de proyecto.
- Ahora puede configurar las políticas de control de recursos (RCP) y las políticas de control de servicios (SCP) para aplicar barreras personalizadas en su organización. Anteriormente, AWS gestionaba los RCP y los SCP en su nombre. Puede modificar esas políticas después de activar las funciones avanzadas. Para obtener más información, consulte Eliminar las políticas de la organización.

Al activar las funciones avanzadas, los siguientes cambios también se aplican a su AWS organización:

- Si tienes un límite de gasto para alguna de tus AWS cuentas, se elimina. Se reactivarán todos los proyectos que estén actualmente en pausa. No puedes crear un límite de gasto si activas las funciones avanzadas. En su lugar, tiene acceso a todo el conjunto de herramientas de Billing and Cost Management. Esto incluye establecer presupuestos, descargar los informes del explorador de costes y detectar gastos inusuales mediante la detección de anomalías en los AWS costes. Puede utilizar estas herramientas avanzadas para analizar, organizar, planificar y optimizar sus costes.
- Puede acceder a todos los AWS servicios. Los servicios disponibles se enumeran enthe section called “Servicios de AWS no es compatible con nuestro nuevo AWS experiencia”. Debe planificar su arquitectura y consultar la documentación del servicio antes de habilitar estos servicios. Además, Agent Toolkit proporciona muchas habilidades para trabajar con estos servicios.
- Obtendrá acceso a regiones adicionales Regiones de AWS y optativas y a funciones multirregionales. Multi-Region la arquitectura mejora la resiliencia de sus cargas de trabajo. Le recomendamos que planifique cómo restringirá y auditará su presencia regional. Es importante que te asegures de que los recursos que crees solo estén presentes en las regiones que piensas utilizar.
- Puede desactivar el administrador de funciones de IAM para cada miembro Cuenta de AWS de su organización. El administrador de funciones de IAM es una configuración de cuenta opcional que aprovisiona automáticamente las funciones, por lo que ni tú ni tus empleados necesitáis configurarlas. Para obtener más información, consulte Cómo habilitar y deshabilitar el administrador de roles (consola).
- Puede utilizar IAM Access Analyzer.

Al activar las funciones avanzadas, los siguientes cambios también se aplican a la experiencia de usuario:

- Anteriormente, Consola de administración de AWS mostraban una vista simplificada con un menú que se utilizaba para cambiar de un proyecto a otro y acceder a AWS la configuración. Se Consola de administración de AWS amplía para incluir funciones adicionales, como el selector de regiones, los servicios adicionales y la configuración de un color para la cuenta al que puedas acceder para distinguirlos visiblemente. Para obtener más información, consulta Características de la consola.
- Ahora también puede hacer lo siguiente:
  - Deshabilite la compatibilidad con consolas multisesión.

- Designa tu AWS cuenta como compatible con la HIPAA o la SEC.
- Usa AWS Marketplace.
- Obtenga créditos adicionales con AWS Activate.
- Trabaje con un compañero AWS de formación.
- Compra una suscripción a AWS Skill Builder Team.
- Inscríbase en un acuerdo empresarial con AWS.
- Cree un contrato de servicios profesionales.
- Únase a AWS Partner Network.

Proyecte las cuentas después de activar las funciones avanzadas

Cada proyecto que hayas creado en AWS Configuración contiene una Cuenta de AWS, denominada cuenta de proyecto. Cada cuenta de proyecto es propiedad de un AWS Builder ID, en lugar de la dirección de correo electrónico del usuario raíz. Cuando activas las funciones avanzadas, las cuentas de tus proyectos se convierten en cuentas de miembros de tu organización y tu AWS Builder ID sigue siendo el propietario de ellas, aunque cambies más adelante tu fuente de identidad. Tu ID de AWS creador también es propietario de la cuenta de administrador delegado de Identity que se AWS crea al activar las funciones avanzadas.

Como una cuenta de proyecto no tiene una dirección de correo electrónico de usuario raíz, funciona de forma diferente a las demás cuentas de miembros de la organización:

- La dirección de correo electrónico que muestra la AWS Organizations consola para una cuenta de proyecto es un marcador de posición que se AWS genera. Las `GetPrimaryEmail` operaciones`DescribeAccount`, `ListAccounts` `ListAccountsForParent``ListDelegatedAdministrators`, y devuelven el mismo marcador de posición. No es una dirección de correo electrónico que puedas usar o cambiar.
- No puedes actualizar la dirección de correo electrónico del usuario raíz de una cuenta de proyecto. Las llamadas a `StartPrimaryEmailUpdate` o `AcceptPrimaryEmailUpdate` para una cuenta de proyecto fallan y se `AccessDeniedException` produce un error, incluso cuando la persona que llama tiene los permisos necesarios.
- No puedes iniciar sesión en una cuenta de proyecto como usuario root ni recuperar su contraseña de usuario root.
- No puedes eliminar una cuenta de proyecto de tu organización, ni tampoco puede salir de ella ni unirse a otra organización. Si `RemoveAccountFromOrganization` solicitas una cuenta de

proyecto, la llamada fallará y aparecerá un `ConstraintViolationException` error que indica que la cuenta es propiedad de un Builder ID.

Para dejar de usar una cuenta de proyecto, ciérrala desde tu cuenta de administración. Como no puedes eliminar cuentas de proyectos de tu organización, solo puedes eliminarlas después de que todas las cuentas de proyecto, incluida la cuenta de administrador delegado de Identity, se hayan cerrado permanentemente. AWS cierra permanentemente una cuenta cuando finaliza el período de 90 días posterior al cierre.

Las cuentas de los miembros que cree en su organización después de activar las funciones avanzadas tienen una dirección de correo electrónico de usuario raíz y estas diferencias no se aplican a ellas. Si necesitas una cuenta cuya dirección de correo electrónico de usuario raíz puedas cambiar o que puedas eliminar de tu organización más adelante, crea una nueva cuenta de miembro y transfiere tus recursos a ella.

¿Cómo lo hará AWS ¿Cambiará la configuración después de activar las funciones avanzadas?

Tras activar las funciones avanzadas, AWS la configuración estará disponible siempre que utilices AWS Builder ID como fuente de identidad. AWS Solo se podrá acceder a la configuración desde https://settings.aws.com. No podrás acceder a ella desde Consola de administración de AWS. AWS La configuración proporcionará enlaces para administrar tu cuenta mediante tu cuenta de administración. Con tu cuenta de administración, puedes acceder a las siguientes Consola de administración de AWS ubicaciones desde la AWS configuración. Utilice la cuenta de administración únicamente para realizar tareas administrativas, como:

- Acceda a la consola de Billing and Cost Management para ver su información de facturación.
- Acceda a la consola de la AWS organización para modificar los SCP y RCP que rigen su organización.
- Acceda a la consola AWS Account Access Manager para modificar el acceso detallado a las identidades de sus empleados.
- Acceda al Centro de identidades de IAM para cambiar la fuente de identidad.

Utilice la cuenta de administración para realizar estas tareas. Si bien también tendrás acceso al correo electrónico y la contraseña del usuario raíz, te recomendamos que solo utilices tus credenciales de usuario raíz para acceder de emergencia a tu cuenta.

También puedes usar la AWS configuración para acceder a AWS las cuentas de tu organización y a cualquier proyecto que se comparta contigo.

Si quieres crear funciones personalizadas y acceder a ellas desde la AWS configuración de tus cuentas, debes establecer la duración de la sesión en 12 horas.

Si tienes acceso a un proyecto como miembro del equipo, puedes verlo y acceder a él de la misma forma que antes de activar las funciones avanzadas. Los proyectos que compartas contigo no se verán afectados si activas las funciones avanzadas para tu propia cuenta de administración y AWS organización.

¿Puedo seguir creando un proyecto en AWS ¿Configuración después de activar las funciones avanzadas?

No puede crear un proyecto en su AWS organización actual después de activar las funciones avanzadas. Debe crear una cuenta de miembro en su organización.

Puede crear una nueva AWS organización gestionada con valores predeterminados preconfigurados. Para ello, crea un nuevo proyecto en AWS Configuración. A continuación, puedes crear proyectos adicionales e invitar a los miembros del equipo a colaborar. También puedes activar funciones avanzadas para esta cuenta de administración.

El nuevo entorno preconfigurado al que accedas no tendrá conexión con la AWS organización anterior que se creó cuando te registraste por AWS primera vez.

Cómo prepararse para activar las funciones avanzadas

Se recomienda hacer lo siguiente antes de activar las funciones avanzadas:

- Informe a todos los miembros de su equipo de que va a activar las funciones avanzadas. A menos que modifiques alguna configuración, los miembros de tu equipo tendrán el mismo acceso a los proyectos, pero Consola de administración de AWS cambiarán de la vista simplificada a una vista que muestra las regiones y proporciona acceso a más servicios. Si más adelante cambias la fuente de identidad o agregas nuevos SCP o RCP, comunícaselo a tus empleados, ya que esos cambios pueden afectar a la forma en que inician sesión y a qué pueden acceder.
- Consulta los gastos de todos tus proyectos actuales y observa si alguno de ellos tiene costes que fluctúen de forma significativa. Sin límite de gasto, serás responsable de todos los costes en los que incurran tus recursos. Le recomendamos que elimine o ponga en pausa los recursos inactivos antes de activar las funciones avanzadas.

- Planifique los cambios que realizará en sus AWS organizaciones e investigue las mejores prácticas. Si planea crear recursos de otra forma Región de AWS, modifique la política de control de servicios que se aplica a todos los usuarios para restringirlos Regiones de AWS. Debe modificar el StatementID `RegionFloor` para incluir cualquier región nueva. Para obtener más información, consulte Políticas de control de servicios para proyectos.
- Si has seguido los pasos descritosConecta una herramienta de codificación de IA, tu herramienta de IA solo incluye el contexto de la nueva experiencia. AWS Esto puede causar problemas a medida que vaya desarrollando el uso de funciones avanzadas. Le recomendamos lo siguiente:
  - Elimine el `aws-starter-rules.md` archivo de la ubicación en la que lo guardó. El archivo de reglas se guardó en función del agente. Para obtener más información, consulte Dónde colocar el archivo de reglas.

¿Cómo activar las funciones avanzadas

Puedes activar las funciones avanzadas en los AWS ajustes. La activación no se puede revertir.

Para activar funciones avanzadas

1. Abre AWS Configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Proyectos.
3. En Acciones, selecciona Explorar funciones avanzadas.

   Como la activación no se puede revertir, proporcionaremos más tiempo para explorar y aprender sobre el proceso de activación.
4. Cuando esté listo para la activación, haga lo siguiente:

   a. En Nombre del equipo, introduce un nombre de equipo. Es el nombre de la instancia del IAM Identity Center que se utiliza para almacenar las identidades de sus empleados. Sus empleados verán este nombre.

   b. En Elegir la dirección de correo electrónico de la cuenta de administración, elige una dirección de correo electrónico. Esta dirección de correo electrónico se utiliza para acceder a la cuenta de administración y realizar tareas. Si utilizas una dirección de correo electrónico diferente, la dirección de correo electrónico del AWS Builder ID seguirá teniendo acceso a la cuenta de administración desde la AWS Configuración, siempre y cuando sigas utilizando el AWS Builder ID como fuente de identidad.

c. Complete el proceso de verificación de la dirección de correo electrónico de la cuenta de administración.

d. Selecciona Revisar y completar la activación.

e. Confirme su elección y seleccione activar. Si lo hace, no podrá revertir su cuenta.

¡Enhorabuena, has activado AWS las funciones avanzadas!

Después de activar las funciones avanzadas

Tras activar las funciones avanzadas, puede hacer lo siguiente:

- Gestione los miembros de la fuerza
- Cambiar la fuente de identidad de AWS ID de creador
- Eliminar las políticas de la organización
- Crea una unidad organizativa
- Actívala o desactiva Regiones de AWS en tu cuenta
- Cree funciones de IAM

Establezca una contraseña de usuario root para su cuenta de administración

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Después de activar las funciones avanzadas, tu cuenta de administración ahora usa una dirección de correo electrónico raíz para la recuperación de la cuenta. Si bien puedes recuperar el acceso a tu ID de AWS Builder mediante las opciones de autoservicio para recuperar el acceso, ahora puedes recuperar el acceso a tu cuenta de administración con las credenciales de usuario root. Para acceder al usuario root, debes crear una contraseña de usuario root. Además, le recomendamos que active la autenticación multifactor (MFA) para mejorar la seguridad del usuario root.

Para establecer una contraseña de usuario raíz

1. Abra la consola AWS de administración y elija Iniciar sesión con el correo electrónico del usuario root.
2. En Dirección de correo electrónico, introduzca la dirección de correo electrónico del usuario raíz.

   Esta es la dirección de correo electrónico que configuró para la cuenta de administración al activar las funciones avanzadas.
3. Elija Forgot your password? (¿Ha olvidado su contraseña?).

   El proceso de restablecimiento de la contraseña también sirve para configurar la contraseña de usuario root después de activar las funciones avanzadas.
4. Introduzca la dirección de correo electrónico asociada a la cuenta.
5. Introduce el texto del CAPTCHA y selecciona No soy un robot.
6. Comprueba el correo electrónico asociado a ti Cuenta de AWS para ver si hay algún mensaje de Amazon Web Services. El correo electrónico procederá de una dirección que termina en `@verify.signin.aws`. Siga las instrucciones del correo electrónico para establecer una contraseña de usuario root. Si no ve el correo electrónico en su cuenta, compruebe la carpeta de spam. Si ya no tienes acceso al correo electrónico, consulta No tengo acceso al correo electrónico de mi AWS cuenta en la Guía del AWS Sign-In usuario.

Una vez que hayas establecido la contraseña del usuario raíz, podrás recuperar el acceso a tu cuenta. A continuación, siga las instrucciones de Multi-factor autenticación para el usuario raíz de la AWS cuenta para activar el MFA en sus credenciales raíz.

Utiliza al usuario raíz únicamente para recuperar tu cuenta o cuando sea necesario para realizar tareas que requieran credenciales de usuario raíz. Para el trabajo diario, inicia sesión con tu fuente de identidad, como AWS Builder ID.

Gestione los miembros de la fuerza

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Una vez que hayas activado las funciones avanzadas, puedes invitar a nuevos miembros de la fuerza laboral o eliminar a los miembros existentes. Esto incluye añadir tu fuerza laboral actual a nuevas AWS cuentas. La siguiente información es solo para AWS las organizaciones que utilizan AWS Builder ID como fuente de identidad. Si usa un proveedor de identidad (IdP) externo, administra su fuerza laboral en esos proveedores de identidad. Si usa el directorio de Identity Center, use la documentación que se describe en Administrar usuarios en el directorio de Identity Center.

Para invitar a nuevos miembros de la fuerza laboral

1. Abra AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Proyectos.
3. Visita la AWS consola de tu cuenta de administrador de identidad delegada.
4. Desde la AWS página de inicio de la consola, búscala **`IAM Identity Center`** y selecciónala.
5. En la página de usuarios de la consola de IAM Identity Center, seleccione Invitar a un nuevo miembro del equipo.
6. En Correo electrónico, introduzca una dirección de correo electrónico o una lista de direcciones de correo electrónico. Separe las direcciones de correo electrónico con comas (,) o punto y coma (;).
7. Seleccione Send invitation (Enviar invitación).

Para conceder a un nuevo miembro de la fuerza laboral acceso a AWS cuentas

Una vez que el miembro de la fuerza laboral acepte su invitación, debe configurar AWS las cuentas a las que tiene acceso.

Otorgue todos los permisos a una cuenta que haya creado antes de activar las funciones avanzadas

1. Identifica el ID de la cuenta a la que quieres conceder acceso. Para encontrar el ID de la cuenta, consulta Ver los identificadores de la AWS cuenta.
2. En el panel de navegación principal, selecciona Grupos.
3. Seleccione el nombre del grupo que comience con el ID de cuenta que identificó.
4. Selecciona Añadir usuarios al grupo.
5. Seleccione el usuario que desee añadir.
6. Selecciona Añadir 1 usuario.

Otorgue permisos personalizados a uno nuevo o existente AWS inscrita

El acceso personalizado se configura en el Administrador de acceso a la AWS cuenta. Para obtener más información, consulte Administrar el acceso a AWS las cuentas.

> **Note**
>
> Si quieres crear funciones personalizadas y conceder acceso a ellas desde la AWS configuración, debes establecer la duración de la sesión en 12 horas.

Para eliminar a los miembros de la fuerza laboral

1. Abra AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Proyectos.
3. En Acciones, selecciona Administrar equipo.

   Esto abrirá el centro de identidad de IAM.
4. En la página de usuarios de la consola del IAM Identity Center, seleccione un miembro del equipo y, a continuación, seleccione Eliminar.
5. Confirme su elección y seleccione Eliminar.

El miembro del equipo perderá inmediatamente todo acceso a tu AWS organización.

Estos pasos le muestran cómo administrar a los miembros de su fuerza laboral accediendo primero a AWS la Configuración. Sin embargo, puede iniciar sesión Consola de administración de AWS con su cuenta de administrador delegado y acceder al Centro de identidad de IAM o a la consola de IAM para gestionar los miembros de su plantilla.

Cambiar la fuente de identidad de AWS ID de creador

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Después de activar las funciones avanzadas, puedes cambiar tu fuente de identidad desde AWS Builder ID. Si cambias tu fuente de identidad de AWS Builder ID, nunca podrás volver a utilizar AWS Builder ID como fuente de identidad para tu AWS organización. Cambiar la fuente de identidad cambia la forma en que sus empleados inician sesión. Tu ID de AWS constructor sigue siendo el propietario de tus cuentas de proyecto.

Para cambiar tu fuente de identidad desde AWS ID de creador

1. Abre AWS Configuración en https://settings.aws.com.
2. En el panel de navegación principal, selecciona Proyectos.
3. En Administrar esta organización, elija Cambiar fuente de identidad.

   Esto abrirá el centro de identidad de IAM.
4. En la página de configuración de la consola del IAM Identity Center, seleccione Acciones y, a continuación, Cambiar fuente de identidad.
5. En Elegir fuente de identidad, se seleccionará AWS Builder ID. Elija una nueva fuente y, a continuación, elija Siguiente.
6. Si va a cambiar a Active Directory, elija el directorio disponible en el menú de la página siguiente. Si vas a cambiarte a un proveedor de identidad externo, te recomendamos que sigas los pasos que se indican en Cómo conectarse a un proveedor de identidad externo.
7. Revisa y confirma los cambios. Deberás seleccionar todas las casillas de verificación para confirmar que entiendes los cambios en tu organización.
8. Confirme su elección y elija Cambiar fuente de identidad.

Estos pasos te muestran cómo cambiar tu fuente de identidad accediendo primero a AWS la Configuración. Sin embargo, puedes iniciar sesión Consola de administración de AWS con tu cuenta de administrador delegado y acceder al Centro de identidades de IAM para cambiar tu fuente de identidad.

Eliminar las políticas de la organización

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Después de activar las funciones avanzadas, puede modificar las políticas de control de recursos (RCP) y las políticas de control de servicios (SCP) para cambiar la gobernanza de su AWS organización. Algunas políticas organizativas AWS administradas se eliminan al activar las funciones avanzadas. Para obtener más información, consulte Políticas gestionadas para su organización. La siguiente información es solo para AWS las organizaciones que utilizan AWS Builder ID como fuente de identidad. Si usas otra fuente, sigue los pasos que se indican en Actualizar una política.

Para modificar una política de control de servicios (SCP)

1. Abra la AWS configuración en. https://settings.aws.com
2. En el panel de navegación principal, seleccione Proyectos.
3. En Administrar esta organización, elige Administrar políticas.

   Esto abrirá la AWS Organizations consola.
4. Seleccione la página de políticas de control de servicios.
5. Elija el nombre de la política que desea actualizar.
6. En la página de detalles de la política, elija Editar política.
7. Realice una de las siguientes modificaciones, o todas:

   - Puede cambiar el nombre de la política introduciendo un nuevo nombre en Nombre de la política.
   - Puede cambiar la descripción ingresando texto nuevo en Policy description (Descripción de la política).
   - Puede editar el texto de la política editando la política en formato JSON en el panel izquierdo. O bien, puede elegir una declaración en el editor de la derecha y modificar sus elementos utilizando los controles. Para obtener más detalles acerca de cada control, consulte la Creación de un procedimiento SCP que se muestra anteriormente en este tema.
8. Cuando haya finalizado, elija Save changes (Guardar cambios).

Para modificar una política de control de recursos (RCP)

1. Abra la AWS configuración en. https://settings.aws.com
2. En el panel de navegación principal, seleccione Proyectos.
3. En Administrar esta organización, elige Administrar políticas.

   Esto abrirá la AWS Organizations consola.

4. Seleccione la página de políticas de control de recursos.
5. Elija el nombre de la política que desea actualizar.
6. En la página de detalles de la política, elija Editar política.
7. Realice una de las siguientes modificaciones, o todas:

   - Puede cambiar el nombre de la política introduciendo un nuevo nombre en Nombre de la política.
   - Puede cambiar la descripción ingresando texto nuevo en Policy description (Descripción de la política).
   - Puede editar el texto de la política editando la política en formato JSON en el panel izquierdo. O bien, puede elegir una declaración en el editor de la derecha y modificar sus elementos utilizando los controles. Para obtener más detalles acerca de cada control, consulte la Creación de un procedimiento RCP que se muestra anteriormente en este tema.
8. Cuando haya finalizado, elija Save changes (Guardar cambios).

En estos pasos, se muestra cómo modificar las políticas de la organización según AWS la configuración. Sin embargo, puedes iniciar sesión Consola de administración de AWS con tu cuenta de administración y acceder a la AWS Organizations consola para modificar estas políticas.

Cierra tu cuenta en AWS Configuración

> **Warning**
>
> Actualmente estamos lanzando nuestra nueva experiencia a un número limitado de clientes. Es posible que aún no puedas acceder a esta experiencia.

Si ya no necesitas la organización y todos los proyectos almacenados en ella, puedes cerrar tus proyectos, cerrar tu cuenta de administración y eliminar tu ID de AWS Builder.

Para asegurarte de que ya no se te cobre por AWS los recursos que consumes, debes cerrar tus proyectos y cerrar la cuenta de administración de tu organización, pero no tienes que cerrar tu AWS perfil. Tu ID de AWS constructor asociado a ella es gratis.

Tras cerrar tu cuenta de administración, puedes volver a abrirla en un plazo de 90 días a partir del día en que la cerraste. El tiempo transcurrido entre el día en que cerró la cuenta de administración y el momento en que la cierra AWS permanentemente es el período posterior al cierre.

Qué necesita saber antes de cerrar su cuenta de administración

Antes de cerrar su cuenta de administración, debe tener en cuenta lo siguiente:

- Al cerrar un proyecto, tenga en cuenta las consideraciones contenidas enLo que necesita saber antes de cerrar su proyecto.
- Debe cerrar todos los proyectos antes de poder cerrar su cuenta de administración.
- Debes cerrar tu cuenta de administración antes de eliminar tu ID de AWS constructor.
- Tras cerrar tu cuenta de administración, puedes volver a abrirla en un plazo de 90 días a partir del día en que la cerraste. El tiempo transcurrido entre el día en que cerró la cuenta de administración y el momento en que la cierra AWS permanentemente es el período posterior al cierre.
- Puede volver a abrir su cuenta durante el periodo posterior al cierre.
- No puedes usar la misma dirección de correo electrónico que estaba registrada en tu organización en el momento del cierre como correo electrónico principal de otra organización. Si quieres usar la misma dirección de correo electrónico para otra organización mientras utilizas Registrarse en AWS (nueva), te recomendamos que la actualices antes del cierre. Para obtener más información, consulte Cambia tu dirección de correo electrónico en AWS Configuración.
- Si has habilitado la autenticación multifactor (MFA) en tu cuenta de administración y has configurado un dispositivo de MFA, la MFA no se eliminará automáticamente al cerrar la cuenta de administración. Si decide dejar MFA activada durante el periodo de 90 días posterior al cierre, mantenga activo el dispositivo MFA hasta que haya caducado el periodo posterior al cierre, por si necesita acceder a la cuenta durante ese tiempo. Tenga en cuenta que los dispositivos con token TOTP de equipo no se pueden asociar a otro usuario luego del cierre permanente de su cuenta. Si quieres usar el token TOTP de hardware con otro usuario más adelante, tienes la opción de desactivar el dispositivo MFA de hardware antes de cerrar la cuenta de administración.

Cerrar un proyecto

Para cerrar sus proyectos, consulteCerrar un proyecto en AWS Configuración.

Cierre su cuenta de administración

Para cerrar tu cuenta de administración

1. Abre AWS la configuración en https://settings.aws.com.
2. En el panel de navegación principal, elija Proyecto.

3. En Acciones, elija Cerrar cuenta de administración.
4. Confirme su elección y elija Cerrar cuenta de administración.

Elimine su AWS ID de creador

La eliminación de su ID de AWS constructor tendrá como resultado lo siguiente:

- Pérdida de acceso: además de tu proyecto y organización, ya no podrás acceder a ninguna de AWS las herramientas y servicios a los que antes accedías a través de AWS Builder ID.
- Eliminación de contenido: todo el contenido restante asociado únicamente a tu ID de AWS Builder se eliminará y ya no podrás acceder a tu contenido ni recuperarlo de las aplicaciones que utilicen tu ID de AWS Builder.
- Eliminación de la información personal: se eliminará cualquier información personal que haya proporcionado en relación con la creación y administración de su ID de AWS Builder, excepto la que AWS pueda conservar la información personal según lo exija o permita la ley, como los registros de su solicitud de eliminación o los datos en un formulario que no lo identifique.

Puedes obtener más información sobre cómo gestionamos tu información en el Aviso AWS de privacidad. Puede actualizar sus preferencias de AWS comunicación o cancelar su suscripción visitando el Centro de preferencias de AWS comunicación.

Los inicios de sesión existentes permanecen sin cambios: si utilizas un inicio de sesión como el de Google o Apple, al eliminar tu ID de AWS Builder no se elimina nada relacionado con tu cuenta de inicio de sesión.

Para eliminar tu AWS ID de creador

1. Abre AWS la configuración en https://settings.aws.com.

   Aunque hayas eliminado tu cuenta de administración, puedes iniciar sesión.
2. En el panel de navegación principal, selecciona Administrar perfil.
3. Para ver la información del perfil, selecciona Administrar perfil.

   Se te redirigirá a tu perfil de AWS Builder ID.
4. En el panel de navegación principal, selecciona Privacidad y datos.
5. Para Eliminar tu ID de AWS constructor, selecciona Eliminar tu ID de AWS constructor.

6. Confirme la elección y elija Eliminar.

Registrarse en AWS (avanzado)

Si eres nuevo en AWS, el primer paso es registrarte en un Cuenta de AWS. Al seguir la información de Registrarse AWS (avanzado), AWS crea una cuenta en la que tienes el control total de la configuración de la cuenta y donde se almacena tu contenido. Utilice esta opción si tiene cargas de trabajo reguladas, como HIPAA o FedRAMP.

Para comparar este registro con Sign up for AWS (nuevo), consulte. Compara las opciones de registro

Para suscribirte a una Cuenta de AWS, tendrás que proporcionar la siguiente información:

- Dirección de correo electrónico de usuario raíz: esta dirección de correo electrónico se utiliza como nombre de inicio de sesión para el usuario raíz y es necesaria para la recuperación de la cuenta. Debe poder recibir los mensajes de correo electrónico enviados a esta dirección. Para poder realizar determinadas tareas, debe comprobar que tiene acceso al correo electrónico enviado a esta dirección.
- AWS nombre de la cuenta: el nombre de la cuenta aparece en varios lugares, como en la factura, y en consolas como el panel de control de Billing and Cost Management y la AWS Organizations consola. Le recomendamos que utilice una forma estándar de asignar nombres a sus cuentas, de modo que los nombres sean fáciles de reconocer. En el caso de las cuentas de las empresas, considere la posibilidad de utilizar un estándar de nomenclatura, como organización, objetivo, entorno (por ejemplo, AnyCompanyauditoría, producción). Para cuentas personales, considere la posibilidad de utilizar un estándar de nomenclatura, como nombre-apellido-propósito (por ejemplo, paulo-santos-cuentadeprueba).
- Dirección: si su dirección de contacto y facturación se encuentra en la India, el acuerdo de usuario de su cuenta es con Amazon Web Services India Private Limited (AWS India), un AWS vendedor local en la India. Debe proporcionar su CVV como parte del proceso de verificación. Es posible que también tenga que introducir una contraseña de un solo uso, según su banco. AWS India cobra 2 INR a tu método de pago como parte del proceso de verificación. AWS India reembolsa los 2 INR una vez finalizada la verificación.
- Número de teléfono: este número se usa para verificar la identidad y confirmar la propiedad de la cuenta. Debe poder recibir llamadas y mensajes SMS a este número de teléfono.

> **Important**
>
> Si esta cuenta es para una empresa, utilice un número de teléfono corporativo para que su empresa pueda mantener el acceso Cuenta de AWS incluso cuando un empleado cambie de puesto o deje la empresa.

Paso 1: cree su cuenta

Estas instrucciones son para crear un Cuenta de AWS exterior de la India. Para crear una cuenta en la India, consulte Crea un Cuenta de AWS por AWS India. Para crear una cuenta que forme parte de una organización administrada por AWS Organizations, consulte Crear una cuenta de miembro en una organización en la Guía del AWS Organizations usuario.

Consola de administración de AWS

Para crear una Cuenta de AWS

1. Abra la página Inscribirse en AWS.
2. Introduzca la dirección de correo electrónico y el Cuenta de AWS nombre del usuario raíz y, a continuación, seleccione Verificar dirección de correo electrónico. Esto envía un código de verificación a tu dirección de correo electrónico.

   > **Important**
   >
   > Si esta cuenta es para una empresa, utilice una lista de distribución corporativa segura (por ejemplo`it.admins@example.com`) para que su empresa pueda conservar el acceso Cuenta de AWS incluso cuando un empleado cambie de puesto o deje la empresa. Como la dirección de correo electrónico se puede utilizar para restablecer las credenciales del usuario raíz de la cuenta, proteja el acceso a esta lista o dirección de distribución.

3. Introduzca su código de verificación y, a continuación, seleccione Verificar.
4. Introduzca una contraseña segura para el usuario raíz, confírmela y, a continuación, pulse Continuar. AWS requiere que la contraseña cumpla las siguientes condiciones:

   - Debe tener 8 caracteres como mínimo y 128 como máximo.

- Debe incluir, como mínimo, tres de estos tipos de caracteres combinados: mayúsculas, minúsculas, números y símbolos ! @ # $ % ^ & * () <> [] {} | _+-=.
- No debe ser idéntica a su Cuenta de AWS nombre o dirección de correo electrónico.

5. Elige tu plan de cuenta. Para obtener más información, consulta los planes de nivel gratuito.
6. Introduce tu información de contacto y, a continuación, lee y acepta el Acuerdo de AWS cliente. Asegúrese de entender los términos antes de aceptarlos.

> **Important**
>
> Si esta cuenta es para una empresa, se recomienda introducir un número de teléfono de la empresa en lugar de un número de teléfono personal. Configurar el usuario raíz de la cuenta con una dirección de correo electrónico individual o un número de teléfono personal puede hacer que la cuenta sea insegura.

7. Introduce tu información de facturación. Si quieres usar una dirección de facturación diferente para tus datos AWS de facturación, selecciona Usar una dirección nueva.

   No puede continuar con el proceso de registro hasta que agregue un método de pago válido.
8. Es posible que tengas que confirmar tu identidad:

   a. En el campo del código de país o región, introduce un número de teléfono al que puedas contactar en los próximos minutos.
   b. En Número de teléfono, introduce un número de teléfono al que puedas contactar en los próximos minutos.
   c. Selecciona Enviar SMS.
   d. Cuando el sistema automatizado se ponga en contacto contigo, introduce el código que recibes y, a continuación, selecciona Continuar.
9. Elige uno de los AWS Support planes disponibles. Para obtener una descripción de los planes de soporte disponibles y sus beneficios, consulte Compare Soporte plans.
10. Seleccione Completar el registro. Aparece una página de confirmación que indica que su cuenta se está activando.
11. Busque en su bandeja de correo electrónico y su carpeta de correo no deseado un mensaje que confirme que su organización ha sido activada. La activación suele hacerse en unos minutos, pero en ocasiones puede tardar hasta 24 horas.

12. Después de recibir el mensaje de activación, puede iniciar sesión en el para empezar Consola de administración de AWSa usarlo Servicios de AWS. Para obtener información general sobre cómo administrar la configuración de su cuenta, consulte Configura tu Cuenta de AWS.

    En el caso de Cuentas de AWS gestionar varias veces AWS Organizations, asigne el acceso administrativo a un usuario administrativo en el Centro de identidades de IAM. Para obtener instrucciones, consulte Configurar el Cuenta de AWS acceso para un usuario administrativo del Centro de Identidad de IAM en la Guía del usuario del Centro de Identidad de IAM.

AWS CLI & SDKs

Puede crear cuentas de miembros en una organización que se administre AWS Organizations ejecutando la CreateAccountoperación mientras ha iniciado sesión en la cuenta de administración de la organización.

No puedes crear una operación independiente Cuenta de AWS fuera de una organización mediante una operación AWS Command Line Interface (AWS CLI) o de AWS API.

Paso 2: (recomendado) Instale el AWS CLI

Instálelo AWS CLI siguiendo las instrucciones de Instalación del AWS CLI. Necesita la versión 2.32.0 o posterior.

Puede utilizarla AWS CLI para que un agente administre AWS los recursos en su nombre.

Tras instalar el AWS CLI, utilice el siguiente comando para iniciar sesión mediante programación:

```
aws login
```

De este modo, las credenciales se cambian automáticamente cada 15 minutos, lo que permite que la sesión sea válida durante un máximo de 12 horas sin intervención manual.

Utilice el siguiente comando para comprobar que sus credenciales funcionan:

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

Para obtener más información sobre cómo acceder a su Cuenta de AWS, consulteAccediendo a su Cuenta de AWS.

Paso 3: (recomendado) Configurar el AWS Servidor MCP

El servidor AWS MCP es un servidor administrado que permite a los agentes acceder a él a AWS través del Protocolo de contexto modelo (MCP). Los agentes pueden buscar AWS la documentación y recuperar la información del servicio sin necesidad de autenticación. Para ejecutar llamadas a la AWS API, ejecutar scripts de Python en un entorno aislado o seguir habilidades seleccionadas, los agentes se autentican mediante sus credenciales de IAM existentes. Para obtener más información, consulte ¿Qué es el kit de herramientas para agentes? AWS

Tras completar el proceso de registro, consulte los siguientes temas:

- Relacionado AWS servicios
- Uso de Usuario raíz de la cuenta de AWS
- Accediendo a su Cuenta de AWS
- Planifica tu Cuenta de AWS estructura de gobierno
- Configura tu Cuenta de AWS
- Solucione sus problemas Cuenta de AWS
- Administre las cuentas en India
- Cerrar un Cuenta de AWS
- Vuelva a abrir un Cuenta de AWS

Relacionado AWS servicios

Dependiendo de cómo te inscribas AWS, tendrás acceso a Cuentas de AWS nuestros proyectos. Los proyectos contienen Cuentas de AWS la configuración para compartirlos con otros colaboradores. Para obtener más información, consulte Compara las opciones de registro. En esta sección, explicamos cómo Cuentas de AWS puedes crear con Sign Up for AWS (avanzado) y trabajar sin problemas con los siguientes servicios:

- IAM

  Cuenta de AWS El tuyo está estrechamente integrado con AWS Identity and Access Management (IAM). Puede utilizar IAM con su cuneta para asegurarse de que otras personas que trabajan en la cuenta dispongan de todo el acceso que necesitan para hacer su trabajo. También utilizas IAM para controlar el acceso a todos tus AWS recursos, no solo a la información específica de la cuenta. Es importante que se familiarice con los conceptos principales y las prácticas

recomendadas de IAM antes de avanzar demasiado con la configuración de la estructura de su Cuenta de AWS. Para más información, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

- AWS Organizations

  Si su empresa es grande o tiene probabilidades de crecer, es posible que desee configurar varias AWS cuentas que reflejen la estructura específica de su empresa. AWS Organizations proporciona la infraestructura y las capacidades subyacentes para que pueda crear y administrar sus entornos de cuentas múltiples. Puede combinar sus cuentas existentes en una organización para poder administrar las cuentas de forma centralizada. Puede crear cuentas que se conviertan automáticamente en parte de su organización y puede invitar a otras cuentas a que se unan a su organización. También puede asociar políticas que afecten a algunas o a todas sus cuentas. Para obtener más información, consulte Cuándo se debe usar AWS Organizations.

  Las siguientes acciones de la API relacionadas con la cuenta forman parte de la AWS Organizations API, no de la API de administración de AWS cuentas. Las incluimos aquí porque los clientes suelen buscar estas operaciones en la documentación de administración de cuentas, pero están definidas en el AWS Organizations espacio de nombres.

  - CreateAccount
  - CreateGovCloudAccount
  - DescribeAccount

- AWS Control Tower

  AWS Control Tower proporciona una forma simplificada de configurar y administrar un entorno seguro de múltiples cuentas AWS . AWS Control Tower automatiza la creación de su entorno de cuentas múltiples mediante AWS Organizations la creación de instancias de un conjunto de cuentas iniciales y con algunas protecciones y configuraciones predeterminadas para el entorno. Puede utilizarlo AWS Control Tower para aprovisionar nuevas cuentas Cuentas de AWS en unos pocos pasos y, al mismo tiempo, asegurarse de que las cuentas se ajusten a las políticas de su organización. Para obtener más información, consulte Cuándo se debe usar AWS Control Tower.

Uso de Usuario raíz de la cuenta de AWS

Dependiendo de cómo te registres AWS, tendrás acceso a Cuentas de AWS o a los proyectos. Los proyectos contienen Cuentas de AWS y la configuración para compartir con otros colaboradores. Para obtener más información, consulte Compara las opciones de registro. En esta sección,

explicamos cómo usar el usuario root en una Cuenta de AWS que crees mediante Sign up for AWS (avanzado). El AWS Builder ID es el propietario de cada cuenta de proyecto en lugar de la dirección de correo electrónico del usuario raíz, por lo que no puedes usar el usuario raíz en una cuenta de proyecto, ni siquiera después de activar las funciones avanzadas.

Cuando creas una Cuenta de AWS, empiezas con una identidad de inicio de sesión llamada usuario Cuenta de AWS raíz, que tiene acceso completo a todos Servicios de AWS los recursos. Se recomiendaencarecidamente que no utilice el usuario raíz para las tareas diarias. Para ver las tareas que requieren credenciales de usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Para evitar utilizar el usuario raíz en las tareas diarias, descubra cómo configurar un usuario administrativo en AWS IAM Identity Center. Para obtener recomendaciones de seguridad adicionales para los usuarios raíz, consulte Mejores prácticas para los usuarios raíz Cuenta de AWS.

> **Important**
>
> Cualquier persona que tenga tus credenciales de usuario raíz Cuenta de AWS tiene acceso ilimitado a todos los recursos de tu cuenta, incluida la información de facturación.

Puede cambiar o restablecer la contraseña del usuario raíz y crear o eliminar claves de acceso (ID de clave de acceso y claves de acceso secretas) para su usuario raíz. Para obtener ayuda para iniciar sesión con su usuario root, consulte Iniciar sesión Consola de administración de AWS como usuario root en la Guía del AWS Sign-In usuario.

Accediendo a su Cuenta de AWS

Esta información se refiere al acceso a tu cuenta Cuenta de AWS si te has registrado para AWS usar la función de registro AWS (avanzada) o si has activado las funciones avanzadas de tu cuenta. Para comparar las opciones de registro, consultaCompara las opciones de registro.

Puede acceder a su cuenta Cuenta de AWS de cualquiera de las siguientes maneras:

Consola de administración de AWS

Consola de administración de AWSEs una interfaz basada en un navegador que puede usar para administrar su Cuenta de AWS configuración y sus AWS recursos.

AWS Herramientas de línea de comandos

Con las herramientas de línea de AWS comandos, puede emitir comandos en la línea de comandos del sistema para realizar Cuenta de AWS cualquier AWS tarea. El uso de la línea de comandos puede ser más rápido y cómo que utilizar la consola. Las herramientas de línea de comandos también son útiles si quieres crear scripts que ejecuten AWS tareas. AWS proporciona dos conjuntos de herramientas de línea de comandos:

- AWS Command Line Interface(AWS CLI). Para obtener información sobre la instalación y el uso del AWS CLI, consulte la Guía del AWS Command Line Interface usuario.
- AWS Tools for Windows PowerShell. Para obtener información sobre la instalación y el uso de las herramientas para Windows PowerShell, consulte la Guía del Herramientas de AWS para PowerShell usuario.

AWS SDK

AWS Los SDK constan de bibliotecas y códigos de muestra para varios lenguajes de programación y plataformas (por ejemplo, Java, Python, Ruby, .NET, iOS y Android). Los SDK se encargan de tareas como firmar solicitudes criptográficamente, gestionar los errores y reintentar las solicitudes de forma automática. Para obtener más información sobre los AWS SDK, incluido cómo descargarlos e instalarlos, consulte Tools for Amazon Web Services.

AWS API de consulta HTTPS para administración de cuentas

La API de consulta HTTPS de administración de AWS cuentas le brinda acceso programático a su cuenta Cuenta de AWS y AWS. La API de consulta HTTPS le permite emitir solicitudes HTTPS directamente al servicio. Cuando use la API HTTPS, debe incluir código para firmar digitalmente las solicitudes utilizando sus credenciales. Para obtener más información, consulte Calling the API by making HTTP Query requests.

Planifica tu Cuenta de AWS estructura de gobierno

Esta información trata sobre la planificación de tu estructura de Cuenta de AWS gobierno si te has registrado para AWS usar la función de registro AWS (avanzada) o si has activado funciones avanzadas para tu cuenta. Para comparar las opciones de registro, consultaCompara las opciones de registro.

Si bien es posible que haya empezado su AWS viaje con una sola cuenta, le AWS recomienda configurar varias cuentas a medida que sus cargas de trabajo aumenten en tamaño y complejidad.

Tanto si su empresa es mediana como grande, le conviene crear un plan de estructura de gobernanza que garantice que se satisfagan sus necesidades de datos y carga de trabajo.

En esta sección se describen los beneficios y los servicios de gobierno disponibles AWS para ayudar a habilitar una estructura de gobierno de múltiples cuentas.

Temas

- Ventajas de usar múltiples Cuentas de AWS
- Cuándo se debe usar AWS Organizations
- Cuándo se debe usar AWS Control Tower
- Descripción de los modos de operación de la API

Ventajas de usar múltiples Cuentas de AWS

Esta información trata sobre las ventajas de usar varias funciones Cuentas de AWS si te has registrado para AWS usar la función de registro AWS (avanzada) o si has activado las funciones avanzadas de tu cuenta. Para comparar las opciones de registro, consultaCompara las opciones de registro.

Cuentas de AWS forman el límite de seguridad fundamental en el. Nube de AWS Sirven como contenedor de recursos y proporcionan una capa crítica de aislamiento que es esencial para crear un entorno seguro y bien gobernado. Para obtener más información, consulte Qué es un Cuenta de AWS?.

Separar los recursos en partes separadas le Cuentas de AWS ayuda a respaldar los siguientes principios en su entorno de nube:

- Control de seguridad: las diferentes aplicaciones pueden tener diferentes perfiles de seguridad que requieren políticas y mecanismos de control diferentes. Por ejemplo, es mucho más fácil hablar con un auditor y poder elegir uno Cuenta de AWS que aloje todos los elementos de su carga de trabajo que están sujetos a las normas de seguridad del sector de tarjetas de pago (PCI).
- Aislamiento: un Cuenta de AWS es una unidad de protección de seguridad. Los posibles riesgos y amenazas de seguridad deben contenerse dentro de un Cuenta de AWS sin afectar a los demás. Puede haber diferentes necesidades de seguridad debido a los diferentes equipos o perfiles de seguridad.

- Muchos equipos: los diferentes equipos tienen diferentes responsabilidades y necesidades de recursos. Puede evitar que los equipos interfieran entre sí moviéndolos para que se separen Cuentas de AWS.
- Aislamiento de datos: además de aislar a los equipos, es importante aislar los almacenes de datos en una cuenta. Esto puede ayudar a limitar la cantidad de personas que pueden acceder a ese almacén de datos y administrarlo. Esto ayuda a contener la exposición a datos altamente privados y, por lo tanto, puede ayudar a cumplir con el Reglamento General de Protección de Datos (RGPD) de la Unión Europea.
- Proceso de negocio: las distintas unidades de negocio o productos pueden tener propósitos y procesos completamente diferentes. Con varios Cuentas de AWS, puedes satisfacer las necesidades específicas de una unidad de negocio.
- Facturación: una cuenta es la única forma verdadera de separar los elementos a nivel de facturación. Las cuentas múltiples ayudan a separar los elementos a nivel de facturación entre unidades de negocio, equipos funcionales o usuarios individuales. Puedes seguir unificando todas tus facturas en un único pagador (utilizando la facturación unificada) AWS Organizations y tener las partidas separadas por Cuenta de AWS.
- Asignación de cuotas: las cuotas AWS de servicio se aplican por separado para cada una de ellas Cuenta de AWS. Separar las cargas de trabajo en diferentes Cuentas de AWS les impide consumir cuotas entre sí.

Todas las recomendaciones y procedimientos descritos en este documento cumplen con el AWS Well-Architected Marco. Este marco está diseñado para ayudarlo a diseñar una infraestructura en la nube flexible, resiliente y escalable. Incluso cuando empieza de a poco, le recomendamos que proceda de acuerdo con estas directrices en el marco. Hacerlo puede ayudarlo a escalar su entorno de forma segura y sin afectar sus operaciones en curso a medida que crece.

Gestión de múltiples Cuentas de AWS

Antes de empezar a agregar varias cuentas, querrá desarrollar un plan para administrarlas. Para ello, le recomendamos que utilice AWS Organizations, que es un AWS servicio gratuito para administrar todos los miembros Cuentas de AWS de su organización.

AWS también ofrece AWS Control Tower, que agrega capas de automatización AWS gestionada a las organizaciones y la integra automáticamente con otros AWS servicios como AWS CloudTrail Amazon CloudWatch y otros. AWS Config AWS Service Catalog Estos servicios pueden generar costos adicionales. Para obtener más información, consulte Precios de AWS Control Tower.

Véase también

- Cuándo se debe usar AWS Organizations
- Cuándo se debe usar AWS Control Tower

Cuándo se debe usar AWS Organizations

Esta información indica cuándo utilizarla AWS Organizations si te has registrado para AWS usar la función de registro AWS (avanzada) o si has activado las funciones avanzadas de tu cuenta. Para comparar las opciones de registro, consultaCompara las opciones de registro.

AWS Organizations es un AWS servicio que puede usar para administrar su Cuentas de AWS grupo. Ofrece características como la facturación consolidada, en la que todas las facturas de sus cuentas se agrupan y son administradas por un único pagador. También puede administrar de forma centralizada la seguridad de su organización mediante controles basados en políticas. Para obtener más información al respecto AWS Organizations, consulte la Guía AWS Organizations del usuario.

Acceso de confianza

Cuando las utilizas AWS Organizations para administrar tus cuentas en grupo, la mayoría de las tareas administrativas de la organización solo las puede realizar la cuenta de administración de la organización. De forma predeterminada, esto incluye solo las operaciones relacionadas con la administración de la propia organización. Puedes extender esta funcionalidad adicional a otros AWS servicios habilitando el acceso confiable entre las organizaciones y ese servicio. El acceso confiable otorga permisos al AWS servicio especificado para acceder a la información sobre la organización y las cuentas que contiene. Cuando habilita el acceso de confianza para Account Management, el servicio de Account Management otorga a Organizations y a sus cuentas de administración permisos para acceder a los metadatos, como la información del contacto principal o alternativo, de todas las cuentas de los miembros de la organización.

Para obtener más información, consulte Habilite el acceso confiable para AWS Administración de cuentas.

Administrador delegado

Después de habilitar el acceso confiable, también puedes optar por designar una de tus cuentas de miembro como cuenta de administrador delegado para la administración de AWS cuentas. Esto permite que la cuenta de administrador delegado realice las mismas tareas de administración de metadatos de Account Management para las cuentas de los miembros de su organización que

anteriormente solo podía realizar la cuenta de administración. La cuenta de administrador delegado solo puede acceder a las tareas del servicio de Account Management. La cuenta de administrador delegado no tiene todos los accesos administrativos a la organización que tiene la cuenta de administración.

Para obtener más información, consulte Habilitar una cuenta de administrador delegado para AWS Administración de cuentas.

Políticas de control de servicios

Si formas Cuenta de AWS parte de una organización gestionada por un administrador AWS Organizations, el administrador de la organización puede aplicar políticas de control de servicios (SCP) que pueden limitar lo que pueden hacer las personas principales de las cuentas de los miembros. Una SCP nunca concede permisos; más bien, es un filtro que limita los permisos que puede usar la cuenta de miembro. Un usuario o rol (entidad principal) en una cuenta de miembro solo puede realizar las operaciones que se encuentren en la intersección de lo permitido por las SCP aplicables a la cuenta y las políticas de permisos de IAM asociadas a la entidad principal. Por ejemplo, puede usar los SCP para evitar que la entidad principal de una cuenta modifique los contactos alternativos de su propia cuenta.

Para ver ejemplos de SCP que se aplican a Cuentas de AWS, consulte. Restringir el acceso mediante AWS Organizations políticas de control de servicio

Habilite el acceso confiable para AWS Administración de cuentas

Estas instrucciones explican cómo habilitar el acceso confiable para la administración de AWS cuentas si te registraste para AWS usar el servicio de registro AWS (avanzado) o si activaste las funciones avanzadas de tu cuenta. Para comparar las opciones de registro, consultaCompara las opciones de registro.

Al habilitar el acceso confiable para la administración de AWS cuentas, el administrador de la cuenta de administración puede modificar la información y los metadatos (por ejemplo, los detalles de contacto principales o alternativos) específicos de cada cuenta de miembro en AWS Organizations. Para obtener más información, consulte AWS Account Management and AWS Organizations en la Guía del usuario de AWS Organizations . Para obtener información general sobre cómo funciona el acceso confiable, consulte AWS Organizations Utilización con otros AWS servicios.

Una vez habilitado el acceso de confianza, puede usar el parámetro `accountID` en las operaciones de la API de Account Management que lo admitan. Puede usar este parámetro correctamente solo

si llama a la operación con las credenciales de la cuenta de administración o desde la cuenta de administrador delegado de su organización, si habilita una. Para obtener más información, consulte Habilitar una cuenta de administrador delegado para AWS Administración de cuentas.

Utilice el siguiente procedimiento para habilitar el acceso de confianza para Account Management en su organización.

> **Permisos mínimos**
>
> Para realizar estas tareas, debe cumplir con los siguientes requisitos:
>
> - Puede realizar esto únicamente desde la cuenta de administración de la organización.
> - Su organización debe tener habilitadas todas las características.

Consola de administración de AWS

Para habilitar el acceso confiable para AWS Administración de cuentas

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. Seleccione AWS Account Management en la lista de servicios.
4. Elija Habilitar acceso de confianza.
5. En el cuadro de diálogo Habilitar el acceso confiable para la administración de AWS cuentas, escriba habilitar para confirmarlo y, a continuación, elija Habilitar el acceso confiable.

AWS CLI & SDKs

Para habilitar el acceso confiable para AWS Administración de cuentas

Luego de ejecutar este comando, puede usar las credenciales de la cuenta de administración de la organización para llamar a las operaciones de la API de Account Management que utilizan el parámetro `--accountId` para hacer referencia a las cuentas de miembro en una organización.

- AWS CLI: enable-aws-service-access

En el siguiente ejemplo, se habilita el acceso confiable para la administración de AWS cuentas en la organización de la cuenta llamante.

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

Este comando no genera ningún resultado si se utiliza correctamente.

Habilitar una cuenta de administrador delegado para AWS Administración de cuentas

Estas instrucciones explican cómo habilitar una cuenta de administrador delegado para la administración de AWS cuentas si te registraste para AWS usar el servicio de registro AWS (avanzado) o si has activado las funciones avanzadas de tu cuenta. Para comparar las opciones de registro, consultaCompara las opciones de registro.

Puede registrar una cuenta de administrador delegado por organización para el servicio de administración de AWS cuentas. Tras registrar esta cuenta, los usuarios y los roles de esa cuenta pueden llamar a las operaciones AWS CLI y al AWS SDK del espacio de `account` nombres que pueden funcionar en el modo Organizaciones, mediante la compatibilidad con un parámetro opcional`AccountId`. Esto permite al administrador delegado acceder a las operaciones de la API de administración de AWS cuentas para las cuentas de otros miembros. AWS Organizations

Para registrar una cuenta de miembro en su organización como cuenta de administrador delegado, utilice el siguiente procedimiento.

AWS CLI & SDKs

Cómo registrar una cuenta de administrador delegado para el servicio de Account Management

Puede utilizar los siguientes comandos para habilitar un administrador delegado para el servicio de Account Management.

> **Permisos mínimos**
>
> Para realizar estas tareas, debe cumplir con los siguientes requisitos:
>
> - Puede realizar esto únicamente desde la cuenta de administración de la organización.
> - Su organización debe tener habilitadas todas las características.

- Debe haber habilitado el acceso de confianza para Account Management en su organización.

Debe especificar la siguiente entidad principal de servicio:

```
account.amazonaws.com
```

- AWS CLI: register-delegated-administrator

  En el siguiente ejemplo, se registra una cuenta de miembro de la organización como administrador delegado del servicio de Account Management.

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

  Este comando no genera ningún resultado si se utiliza correctamente.

  Tras ejecutar este comando, puede usar las credenciales de la cuenta 123456789012 para llamar a las operaciones de la API de gestión de cuentas AWS CLI y del SDK que utilizan el `--account-id` parámetro para hacer referencia a las cuentas de los miembros de una organización.

Consola de administración de AWS

Esta tarea no se admite en la consola de administración de cuentas. AWS Solo puedes realizar esta tarea mediante la operación de la API AWS CLI o una operación de API de uno de los AWS SDK.

Restringir el acceso mediante AWS Organizations políticas de control de servicio

Esta información trata sobre la restricción del acceso mediante políticas de control de AWS Organizations servicios si te has registrado para AWS usar la función de registro AWS (avanzada) o si has activado las funciones avanzadas de tu cuenta. Para comparar las opciones de registro, consultaCompara las opciones de registro.

En este tema se presentan ejemplos en los que se muestra cómo utilizar políticas de control de servicio (SCP) en AWS Organizations para restringir lo que pueden hacer los usuarios y roles de las cuentas en su organización. Para obtener más información sobre las políticas de control de servicios, consulte los siguientes temas en la Guía del usuario de AWS Organizations :

- Creating SCPs
- Attaching SCPs to OUs and accounts
- Strategies for SCPs
- SCP policy syntax

Example Ejemplo 1: impedir que las cuentas modifiquen sus propios contactos alternativos

En el siguiente ejemplo, se impide que cualquier cuenta de miembro llame a las operaciones de la API `PutAlternateContact` y `DeleteAlternateContact` en el modo de cuenta independiente. Esto impide que las entidades principales de las cuentas afectadas cambien sus propios contactos alternativos.

JSON

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

Example Ejemplo 2: impedir que una cuenta de miembro modifique contactos alternativos para cualquier otra cuenta de miembro de la organización

En el siguiente ejemplo, se generaliza el elemento `Resource` a "*", lo que significa que se aplica tanto a las solicitudes en modo independiente como a las solicitudes en modo de organizaciones. Esto significa que, incluso la cuenta de administrador delegado para Account Management (si se le aplica la SCP) no puede cambiar ningún contacto alternativo para cualquier cuenta en la organización.

JSON

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

Example Ejemplo 3: impedir que una cuenta de miembro de una UO modifique sus propios contactos alternativos

En el siguiente ejemplo de SCP, se incluye una condición que compara la ruta de organización de la cuenta con una lista de dos unidades organizativas. Esto impide que la entidad principal de cualquier cuenta en las UO especificadas modifique sus propios contactos alternativos.

Cuándo se debe usar AWS Control Tower

Esta información indica cuándo utilizarla AWS Control Tower si te has registrado para AWS usar la función de registro AWS (avanzada) o si has activado las funciones avanzadas de tu cuenta. Para comparar las opciones de registro, consultaCompara las opciones de registro.

AWS Organizations es el servicio fundamental que le permite administrar y proteger de forma centralizada todo AWS su entorno. Un componente crucial de este enfoque AWS Organizations centrado es. AWS Control Tower AWS Control Tower actúa como una consola de administración dentro de las organizaciones y proporciona una forma simplificada de configurar y administrar un AWS entorno seguro y de múltiples cuentas mediante la aplicación de las mejores prácticas prescriptivas.

Este enfoque de mejores prácticas de seguridad proporcionado por AWS Control Tower amplía las capacidades principales de. AWS Organizations AWS Control Tower aplica un conjunto de barreras preventivas y de detección para ayudar a garantizar que su organización y sus cuentas se mantengan alineadas con los estándares de seguridad y cumplimiento recomendados.

Al establecer una AWS Organizations estructura bien diseñada AWS Control Tower, puede implementar rápidamente un entorno escalable, seguro y que cumpla con las normas. AWS Este enfoque centralizado de la administración y el gobierno de la nube es esencial para las empresas que desean aprovechar todo el potencial de la nube y, al Nube de AWS mismo tiempo, mantener los más altos estándares de seguridad y cumplimiento.

Para obtener más información, consulte ¿Qué es AWS Control Tower? en la Guía del usuario de AWS Control Tower .

Descripción de los modos de operación de la API

Esta información trata sobre cómo entender los modos de funcionamiento de las API si te has registrado para AWS usar la función de registro AWS (avanzada) o si has activado las funciones avanzadas de tu cuenta. Para comparar las opciones de registro, consultaCompara las opciones de registro.

Las operaciones de la API que funcionan con los atributos Cuenta de AWS de una A siempre funcionan en uno de los dos modos de funcionamiento:

- Contexto independiente: este modo se usa cuando un usuario o rol de una cuenta accede o cambia un atributo de la cuenta en la misma cuenta. El modo de contexto independiente se usa automáticamente cuando no incluyes el `AccountId` parámetro al llamar a una de las operaciones de administración de cuentas AWS CLI o del AWS SDK.
- Contexto de organizaciones: este modo se usa cuando un usuario o rol en la cuenta de una organización accede o cambia un atributo de cuenta en una cuenta de miembro diferente en la misma organización. El modo de contexto de la organización se usa automáticamente cuando incluyes el `AccountId` parámetro al llamar a una de las operaciones de administración de cuentas

AWS CLI o del AWS SDK. En este modo, solo puede llamar a las operaciones desde la cuenta de administración de la organización o desde la cuenta de administrador delegado para Account Management.

Las operaciones del AWS SDK AWS CLI y del SDK pueden funcionar tanto en el contexto independiente como en el de una organización.

- Si no incluye el parámetro `AccountId`, la operación se ejecuta en el contexto independiente y aplica automáticamente la solicitud a la cuenta que utilizó para realizarla. Esto es cierto independientemente de que la cuenta sea miembro de una organización o no.
- Si incluye el parámetro `AccountId`, la operación se ejecuta en el contexto de organizaciones y funciona en la cuenta de Organizations especificada.
  - Si la cuenta que llama a la operación es la cuenta de administración o la cuenta de administrador delegado del servicio de Account Management, puede especificar cualquier cuenta de miembro de esa organización en el parámetro `AccountId` para actualizar la cuenta especificada.
  - La única cuenta de una organización que puede llamar a una de las operaciones de contacto alternativo y especificar su propio número de cuenta en el parámetro `AccountId` es la cuenta especificada como cuenta de administrador delegado del servicio de Account Management. Cualquier otra cuenta, incluida la cuenta de administración, recibe una excepción `AccessDenied`.
- Si ejecuta una operación en modo independiente, debe tener permiso para ejecutar la operación con una política de IAM que incluya un elemento `Resource` de `"*"` para permitir todos los recursos o un ARN que utilice la sintaxis de una cuenta independiente.
- Si ejecuta una operación en modo de organizaciones, debe tener permiso para ejecutar la operación con una política de IAM que incluya un elemento `Resource` de `"*"` para permitir todos los recursos o un ARN que utilice la sintaxis de una cuenta de miembro en una organización.

Conceder permisos para actualizar los atributos de la cuenta

Como ocurre con la mayoría de AWS las operaciones, se conceden permisos para agregar, actualizar o eliminar atributos de la cuenta Cuentas de AWS mediante políticas de permisos de IAM. Cuando adjunta una política de permisos de IAM a una entidad principal de IAM (ya sea un usuario o un rol), especifica qué acciones puede realizar esa entidad principal, en qué recursos y en qué condiciones.

Las siguientes son algunas consideraciones específicas de Account Management para crear una política de permisos.

Formato de nombre de recurso de Amazon para Cuentas de AWS

- El nombre de recurso de Amazon (ARN) Cuenta de AWS que puede incluir en el `resource` elemento de una declaración de política se elabora de forma diferente en función de si la cuenta a la que desea hacer referencia es una cuenta independiente o una cuenta perteneciente a una organización. Consulte la sección anterior en Descripción de los modos de operación de la API.
  - Un ARN de cuenta para una cuenta independiente:

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

    Debe utilizar este formato cuando ejecuta una operación de atributos de cuenta en modo independiente al no incluir el parámetro `AccountID`.
  - Un ARN de cuenta para una cuenta de miembro en una organización:

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

    Debe utilizar este formato cuando ejecuta una operación de atributos de cuenta en modo de organizaciones e incluye el parámetro `AccountID`.

Claves de contexto para las políticas de IAM

El servicio de Account Management también brinda varias claves de condición específicas del servicio de Account Management que ofrecen un control detallado de los permisos que concede.

`cuenta: AccountResourceOrgPaths`

La clave de contexto `account:AccountResourceOrgPaths` le permite especificar una ruta a través de la jerarquía de su organización hasta una unidad organizativa (UO) específica. Solo las cuentas de miembro incluidas en esa UO cumplen esta condición. El siguiente fragmento de ejemplo restringe la política para que se aplique únicamente a las cuentas que se encuentran en una de las dos UO especificadas.

Como `account:AccountResourceOrgPaths` es un tipo de cadena con varios valores, debe utilizar los operadores de cadena con varios valores `ForAnyValue o ForAllValues`. Además, ten

en cuenta que el prefijo de la clave de condición es`account`, aunque estés haciendo referencia a las rutas a las unidades organizativas de una organización.

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

`cuenta: AccountResourceOrgTags`

La clave de contexto `account:AccountResourceOrgTags` le permite hacer referencia a las etiquetas que se pueden asociar a una cuenta en una organización. Una etiqueta es un par de key/value cadenas que puedes usar para categorizar y etiquetar los recursos de tu cuenta. Para obtener más información, consulte Tag Editor en la Guía del usuario de Grupos de recursos de AWS . Para obtener información sobre el uso de etiquetas como parte de una estrategia de control de acceso basada en atributos, consulte What is ABAC for AWS en la Guía del usuario de IAM. El siguiente fragmento de ejemplo restringe la política para que se aplique únicamente a las cuentas de una organización que tengan la etiqueta con la clave `project` y un valor de `blue` o `red`.

Como `account:AccountResourceOrgTags` es un tipo de cadena con varios valores, debe utilizar los operadores de cadena con varios valores `ForAnyValue o ForAllValues`. Además, ten en cuenta que el prefijo de la clave de condición es`account`, aunque estés haciendo referencia a las etiquetas de la cuenta de miembro de una organización.

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

> **Note**
>
> Solo puede adjuntar etiquetas a una cuenta de una organización. No puedes adjuntar etiquetas a una unidad independiente. Cuenta de AWS

Configura tu Cuenta de AWS

Estas instrucciones muestran cómo configurar Cuenta de AWS si te has registrado para AWS usar la opción de registro AWS (avanzada) o si has activado las funciones avanzadas de tu cuenta. Para comparar las opciones de registro, consultaCompara las opciones de registro.

Esta sección incluye temas que describen cómo administrar su Cuenta de AWS.

> **Note**
>
> Si Cuenta de AWS se creó en la India con Amazon Web Services India Private Limited (AWS India), hay que tener en cuenta otras consideraciones. Para obtener más información, consulte Administre las cuentas en India.

Temas

- Crea un Cuenta de AWS alias
- Activar o desactivar Regiones de AWS en tu cuenta
- Actualiza la facturación de tu Cuenta de AWS
- Actualiza el dirección de correo electrónico del usuario raíz
- Actualizar la contraseña del usuario raíz
- Actualiza tu Cuenta de AWS name
- Actualiza los contactos alternativos de tu Cuenta de AWS
- Actualiza el contacto principal de tu Cuenta de AWS
- Visualización Cuenta de AWS identificadores

Crea un Cuenta de AWS alias

Estas instrucciones explican cómo crear un Cuenta de AWS alias si te registraste para AWS usar la función de registro AWS (avanzada) o si has activado funciones avanzadas para tu cuenta. Para comparar las opciones de registro, consultaCompara las opciones de registro.

Si quieres que la URL de tus usuarios de IAM contenga el nombre de tu empresa (u otro identificador fácil de recordar) en lugar del Cuenta de AWS ID, puedes crear un alias de cuenta.

Para obtener información sobre cómo crear o actualizar un alias de cuenta, consulte Uso de un alias como Cuenta de AWS identificador en la Guía del usuario de IAM.

Activar o desactivar Regiones de AWS en tu cuenta

Esta información trata sobre la activación o desactivación Regiones de AWS de las funciones avanzadas de tu cuenta Cuenta de AWS si te has registrado para AWS usar la función de registro AWS (avanzada) o si has activado las funciones avanzadas de tu cuenta. Para comparar las opciones de registro, consulta. Compara las opciones de registro

An Región de AWS es una ubicación física del mundo en la que hay varias zonas de disponibilidad. AWS Las zonas de disponibilidad constan de uno o más centros de AWS datos discretos, cada uno con alimentación, redes y conectividad redundantes, alojados en instalaciones independientes. Esto significa que cada una Región de AWS está físicamente aislada y es independiente de las demás regiones. Las regiones proporcionar tolerancia a errores, estabilidad y resistencia, y también pueden reducir la latencia. Ejecutar las cargas de trabajo Región de AWS más cerca de los usuarios finales puede mejorar el rendimiento y reducir la latencia. Para consultar un mapa de las regiones disponibles y futuras, consulte Regiones y zonas de disponibilidad. Para obtener más información sobre la arquitectura Regiones de AWS de resiliencia para sus cargas de trabajo, consulte AWS Aspectos básicos de varias regiones.

Regiones de AWS En términos generales, se dividen en dos categorías de disponibilidad para las cuentas:

- Regiones predeterminadas: las regiones lanzadas antes del 20 de marzo de 2019 se encuentran habilitadas de forma predeterminada. Puede crear y administrar recursos en estas regiones predeterminadas inmediatamente después de la activación de su cuenta. Las regiones predeterminadas no se pueden activar ni desactivar.
- Opt-in Regiones: las regiones lanzadas después del 20 de marzo de 2019 están inhabilitadas de forma predeterminada y se denominan regiones de suscripción voluntaria. Las regiones

de suscripción inhabilitadas no se muestran en la barra de navegación de la consola y no puede usarlas para crear cargas de trabajo hasta que no estén habilitadas. Para usar estas regiones opcionales, primero debes habilitarlas en tu. Cuenta de AWS Tras activar una región de suscripción, puede seleccionarla en la barra de navegación, y crear y gestionar los recursos en esa región. Para habilitar una región de suscripción para sus cuentas independientes, consulte Habilitar o deshabilitar una región para cuentas independientes y para habilitar una región de suscripción para sus cuentas de miembro, consulte. Habilitar o deshabilitar una región en su organización

Cuando te registras en una Cuenta de AWS, te AWS recomienda una región de suscripción según el país de tu dirección de contacto. Los clientes de un país con una región de AWS suscripción voluntaria ven una recomendación en la página de información de contacto para habilitar la región de suscripción en ese país. Los clientes de un país que cuenta con una región de suscripción y una región predeterminada, como India, Australia o Canadá, reciben una recomendación para seleccionar la región de suscripción si esta se encuentra más cerca de ellos que la región predeterminada. Después de activar una cuenta, puedes habilitar otras AWS regiones en tu cuenta o elegir deshabilitar la región que habilitaste al registrarte.

Al crear una Cuenta de AWS, tus datos y credenciales de IAM se configuran automáticamente para que funcionen en todas las regiones predeterminadas, lo que permite a las identidades de usuario raíz e IAM con los permisos adecuados acceder a los AWS servicios de estas regiones utilizando sus credenciales existentes. AWS Las regiones opcionales están deshabilitadas de forma predeterminada y los datos y las credenciales de IAM no están disponibles inicialmente en estas regiones, lo que impide el acceso a AWS los servicios de esa región. Cuando decide habilitar una región de suscripción, AWS propaga sus datos y credenciales de IAM a esa región. Una vez finalizada la propagación y habilitada la región de suscripción, las identidades de usuario raíz e IAM podrán acceder a los AWS servicios de la región de suscripción recién habilitada con las mismas credenciales de IAM que utilizan en las regiones predeterminadas.

Cuando deshabilita una región de suscripción, sus credenciales de IAM se desactivan y pierde el acceso de IAM a los recursos de dicha región. Al deshabilitar una región de suscripción no se eliminan los recursos de esa región y los cargos por los recursos (si los hubiera) en esa región de suscripción deshabilitada se siguen acumulando a la tarifa estándar.

> **Important**
>
> La desactivación de una región inhabilita el acceso de IAM a los recursos de la región. Esto no elimina los recursos en cuestión, que siguen generando cargos. Elimine los recursos restantes antes de deshabilitar una región.

AWS agrupa las regiones en particiones. Cada región está exactamente en una partición y cada partición tiene una o más regiones. Las particiones tienen instancias independientes de AWS Identity and Access Management (IAM) y proporcionan un límite fijo entre las regiones de las diferentes particiones. AWS Las regiones comerciales están en la `aws` partición, las regiones de China están en la `aws-cn` partición y AWS GovCloud (US) las regiones están en la `aws-us-gov` partición. En función de la partición en la que haya creado la suya Cuenta de AWS, puede utilizarla Regiones de AWS dentro de esa partición.

- Una cuenta en `aws` partición le brinda acceso a varias regiones de la partición comercial para que pueda lanzar AWS recursos en las ubicaciones que cumplan con sus requisitos. Por ejemplo, podría desear lanzar instancias de Amazon EC2 en Europa, para estar más cerca de sus clientes europeos o para cumplir requisitos legales.
- Una cuenta en la `aws-us-gov` partición le brinda acceso a la región AWS GovCloud (US-West) y a la región AWS GovCloud (US-East). Para obtener más información, consulte AWS GovCloud (US).
- Una cuenta en la partición `aws-cn` proporciona acceso solo a las regiones de Pekín y Ningxia. Para obtener más información, consulte Amazon Web Services en China.

Temas

- Referencia de disponibilidad regional
- Observaciones antes de habilitar o deshabilitar regiones
- Tiempos de procesamiento y límites de solicitudes
- Habilitar o deshabilitar una región para cuentas independientes
- Habilitar o deshabilitar una región en su organización

Referencia de disponibilidad regional

Las siguientes tablas muestran una lista Regiones de AWS por tipo de disponibilidad. Las regiones predeterminadas se activan automáticamente y no se pueden deshabilitar, mientras que las regiones de suscripción deben habilitarse de manera manual para poder usarlas:

Opt-in Regions

Las siguientes regiones son regiones de suscripción que deben estar habilitadas para poder usarlas:

Name	Código	Status
África (Ciudad del Cabo)	`af-south-1`	GA
Asia-Pacífico (Hong Kong)	`ap-east-1`	GA
Asia-Pacífico (Taipéi)	`ap-east-2`	GA
Asia-Pacífico (Hyderabad)	`ap-south-2`	GA
Asia-Pacífico (Yakarta)	`ap-southeast-3`	GA
Asia-Pacífico (Melbourne)	`ap-southeast-4`	GA
Asia-Pacífico (Malasia)	`ap-southeast-5`	GA
Asia-Pacífico (Nueva Zelanda)	`ap-southeast-6`	GA
Asia-Pacífico (Tailandia)	`ap-southeast-7`	GA
Oeste de Canadá (Calgary)	`ca-west-1`	GA
Europa (Zúrich)	`eu-central-2`	GA
Europa (Milán)	`eu-south-1`	GA
Europa (España)	`eu-south-2`	GA
Israel (Tel Aviv)	`il-central-1`	GA
Medio Oriente (EAU)	`me-central-1`	GA

Name	Código	Status
Middle East (Bahrain)	me-south-1	GA
México (centro)	mx-central-1	GA

Default Regions

Las siguientes regiones están habilitadas de forma predeterminada y no se pueden deshabilitar:

Name	Código
Asia-Pacífico (Tokio)	ap-northeast-1
Asia-Pacífico (Seúl)	ap-northeast-2
Asia-Pacífico (Osaka)	ap-northeast-3
Asia-Pacífico (Mumbai)	ap-south-1
Asia-Pacífico (Singapur)	ap-southeast-1
Asia-Pacífico (Sídney)	ap-southeast-2
Canadá (centro)	ca-central-1
Europa (Fráncfort)	eu-central-1
Europa (Estocolmo)	eu-north-1
Europa (Irlanda)	eu-west-1
Europa (Londres)	eu-west-2
Europa (París)	eu-west-3
América del Sur (São Paulo)	sa-east-1
Este de EE. UU. (Norte de Virginia)	us-east-1

Name	Código
Este de EE. UU. (Ohio)	`us-east-2`
Oeste de EE. UU. (Norte de California)	`us-west-1`
Oeste de EE. UU. (Oregón)	`us-west-2`

Para obtener una lista de los nombres de las regiones y sus códigos correspondientes, consulte los puntos de conexión regionales en la Guía de referencia general de AWS . Para obtener una lista de AWS los servicios compatibles en cada región (sin terminales), consulte la lista de servicios AWS regionales.

> **Important**
>
> AWS recomienda usar puntos de enlace regionales AWS Security Token Service (AWS STS) en lugar del punto de enlace global para reducir la latencia. Los tokens de sesión de los AWS STS puntos finales regionales son válidos en todas las AWS regiones. Si utilizas AWS STS puntos de conexión regionales, no necesitas hacer ningún cambio. Sin embargo, los tokens de sesión del AWS STS punto final global (https://sts.amazonaws.com) solo son válidos si Regiones de AWS los habilitas o si están habilitados de forma predeterminada. Si quieres habilitar una nueva región para tu cuenta, puedes usar los tokens de sesión de los AWS STS terminales regionales o activar el AWS STS punto final global para emitir tokens de sesión que sean válidos en todos Regiones de AWS. Los tokens de sesión que son válidos en todas las regiones son más grandes. Si almacena tokens de sesión, estos tokens más grandes podrían afectar a sus sistemas. Para obtener más información sobre cómo funcionan AWS STS los puntos finales con AWS las regiones, consulte Administrar AWS STS en una AWS región.

Observaciones antes de habilitar o deshabilitar regiones

Antes de habilitar o deshabilitar una región, es importante que tenga en cuenta lo siguiente:

- Puede usar todas las regiones de destino de una geografía de inferencia interregional, independientemente de su Region-opt estado. Algunos servicios de IA AWS generativa, como Amazon Bedrock (consulte Aumentar el rendimiento con la inferencia interregional) y Amazon Q Developer (consulte Cross-region Procesamiento en Amazon Q Developer), utilizan inferencias

interregionales. Si utiliza esos servicios, seleccionarán automáticamente la mejor Región de AWS, incluidas las regiones en las que no haya habilitado los recursos y los datos de IAM, dentro de la geografía que ha seleccionado. Esto mejora la experiencia del cliente al maximizar la disponibilidad de los modelos y los cálculos disponibles.

- Puede usar los permisos de IAM para controlar el acceso a las regiones. AWS Identity and Access Management (IAM) incluye cuatro permisos que le permiten controlar qué usuarios pueden habilitar, deshabilitar, obtener y enumerar las regiones. Para obtener más información, consulte AWS: permite habilitar y deshabilitar Regiones de AWS en la Guía del usuario de IAM. También puedes usar la clave de `aws:RequestedRegion` condición para controlar el acceso a un Servicios de AWS . Región de AWS
- La habilitación y deshabilitación de una región es gratuita: no se aplica ningún cargo por habilitar o deshabilitar una región. Solo se le cobrará por los recursos que cree en la nueva región.
- EventBridge Integración con Amazon: puedes suscribirte a las notificaciones de actualización de estado según tu región en. EventBridge Se creará una EventBridge notificación para cada cambio de estado, lo que permitirá a los clientes automatizar los flujos de trabajo.
- Region-opt Estado expresivo: debido a la naturaleza asincrónica de enabling/disabling una región de suscripción voluntaria, hay cuatro estados posibles para una solicitud de aceptación regional:
  - `ENABLING`
  - `DISABLING`
  - `ENABLED`
  - `DISABLED`

  No puede cancelar una suscripción o exclusión si se encuentra en uno de los estados `ENABLING` o `DISABLING`. De lo contrario, se lanzará una `ConflictException`. Una solicitud de aceptación regional completada (Enabled/Disabled) depende del aprovisionamiento de los principales servicios subyacentes. AWS Es posible que algunos AWS servicios no se puedan utilizar de inmediato a pesar de que su estado sea. `ENABLED`

Tiempos de procesamiento y límites de solicitudes

Cuando habilita o deshabilita las regiones, tenga en cuenta las siguientes limitaciones de tiempo y solicitud:

- Habilitar una región tarda entre unos minutos y varias horas en algunos casos: cuando habilita una región, AWS realiza acciones para preparar su cuenta en dicha región, como la distribución de sus

recursos de IAM a la región. Este proceso tarda unos minutos para la mayoría de las cuentas, pero a veces puede tardar varias horas. No puede utilizar la región hasta que este proceso finalice.

- La deshabilitación de una región no siempre está visible de forma inmediata: es posible que los servicios y las consolas estén visibles temporalmente después de deshabilitar una región. La desactivación de una región puede tardar de unos minutos a varias horas en surtir efecto.
- Una sola cuenta puede tener 6 solicitudes de suscripción/exclusión de región en curso en un momento dado: una solicitud equivale a habilitar o deshabilitar una región en particular para una cuenta.
- Las organizaciones pueden tener 50 solicitudes de aceptación regional abiertas en un momento determinado en toda la AWS organización. La cuenta de administración puede tener en cualquier momento 50 solicitudes abiertas pendientes de finalización para su organización. Una solicitud equivale a habilitar o deshabilitar una región concreta para una cuenta.

Habilitar o deshabilitar una región para cuentas independientes

Para actualizar las regiones a las que Cuenta de AWS tiene acceso, siga los pasos del siguiente procedimiento. El siguiente Consola de administración de AWS procedimiento siempre funciona solo en el contexto independiente. Puede utilizarla Consola de administración de AWS para ver o actualizar únicamente las regiones disponibles en la cuenta que utilizó para llamar a la operación.

Consola de administración de AWS

Para activar o desactivar una región de forma independiente Cuenta de AWS

> **Permisos mínimos**
>
> Para realizar los pasos del siguiente procedimiento, un rol o usuario de IAM debe tener los siguientes permisos:
>
> - `account:ListRegions`(es necesario para ver la lista de las que están habilitadas o deshabilitadas actualmente Regiones de AWS y si están habilitadas o deshabilitadas).
> - `account:EnableRegion`
> - `account:DisableRegion`

1. Inicia sesión Consola de administración de AWS como usuario o rol de IAM Usuario raíz de la cuenta de AWS o como usuario o rol con los permisos mínimos.

2. En la parte superior derecha de la ventana, seleccione el nombre de cuenta y, a continuación, seleccione Cuenta.
3. En la página de la cuenta, desplácese hacia abajo hasta la sección Regiones de AWS.
4. Elija la región que desee habilitar o deshabilitar y, a continuación, elija la acción que desee, Activar o Desactivar. Verá una petición para confirmarlo.
5. Si ha elegido la opción Habilitar, revise el texto que se muestra y, a continuación, seleccione Habilitar región.

   Si eligió la opción Deshabilitar, revise el texto que se muestra, escriba **`disable`** para confirmar y, a continuación, seleccione Deshabilitar región.

   Una vez habilitada la región de suscripción, puede seleccionarla en la barra de navegación regional. Para ver los pasos para seleccionar una región, consulte Elegir una región en la barra de navegación en la Consola de administración de AWS y, para ver la configuración de consola específica de la región en su cuenta, consulte Configurar la región predeterminada en la Consola de administración de AWS.

AWS CLI & SDKs

Puedes habilitar, deshabilitar, leer y mostrar el estado de opción regional mediante los siguientes AWS CLI comandos o sus operaciones equivalentes en el AWS SDK:

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

> **Permisos mínimos**
>
> Para realizar los siguientes pasos, debe tener el permiso correspondiente a esa operación:
>
> - `account:EnableRegion`
> - `account:DisableRegion`
> - `account:GetRegionOptStatus`

- `account:ListRegions`

Si utiliza estos permisos individuales, puede conceder a algunos usuarios la capacidad de solo leer la información de opción de región y conceder a otros la capacidad tanto de leer como de escribir.

En el siguiente ejemplo, se habilita una región para la cuenta de miembro especificada en una organización. Las credenciales que se usan deben ser de la cuenta de administración de la organización o de la cuenta de administrador delegado del servicio de Account Management.

Tenga en cuenta que también puede deshabilitar una región con el mismo comando y, a continuación, reemplazar `enable-region` con `disable-region`.

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

Este comando no genera ningún resultado si se utiliza correctamente.

La operación es asíncrona. El siguiente comando le permitirá ver el estado más reciente de la solicitud.

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

Habilitar o deshabilitar una región en su organización

Para actualizar las regiones habilitadas para sus cuentas de miembro AWS Organizations, siga los pasos del siguiente procedimiento.

> **Note**
>
> Las políticas AWS Organizations administradas `AWSOrganizationsReadOnlyAccess` o `AWSOrganizationsFullAccess` se actualizan para permitir el acceso a las API de administración de AWS cuentas, de modo que pueda acceder a los datos de la cuenta desde

la AWS Organizations consola. Para ver las políticas administradas actualizadas, consulta Actualizaciones de las políticas AWS administradas de las organizaciones.

> **Note**
>
> Para poder realizar estas operaciones desde la cuenta de administración o desde una cuenta de administrador delegado en una organización para utilizarlas con las cuentas de los miembros, debe hacer lo siguiente:
>
> - Habilite todas las características en su organización para administrar la configuración en sus cuentas de miembro. Esto le permite al administrador controlar las cuentas de miembro. Esto se establece de forma predeterminada cuando crea la organización. Si su organización está configurada únicamente para la facturación consolidada y desea habilitar todas las características, consulte Enabling all features in your organization.
> - Habilite el acceso confiable para el servicio de administración de AWS cuentas. Para configurarlo, consulte Habilite el acceso confiable para AWS Administración de cuentas.

Consola de administración de AWS

Cómo habilitar o deshabilitar una región en su organización

1. Inicie sesión en la AWS Organizations consola con las credenciales de la cuenta de administración de su organización.
2. En la página Cuentas de AWS, seleccione la cuenta que desea actualizar.
3. Elija la pestaña Configuración de la cuenta.
4. En Regiones, seleccione la región que desea habilitar o deshabilitar.
5. Seleccione Acciones y, a continuación, elija la opción Habilitar o Deshabilitar.
6. Si ha elegido la opción Habilitar, revise el texto que se muestra y, a continuación, seleccione Habilitar región.
7. Si eligió la opción Deshabilitar, revise el texto que se muestra, escriba deshabilitar para confirmar y, a continuación, seleccione Deshabilitar región.

AWS CLI & SDKs

Puedes habilitar, deshabilitar, leer y mostrar el estado de opción regional de las cuentas de los miembros de la organización mediante los siguientes AWS CLI comandos o sus operaciones equivalentes en el AWS SDK:

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

> **Permisos mínimos**
>
> Para realizar los siguientes pasos, debe tener el permiso correspondiente a esa operación:
>
> - `account:EnableRegion`
> - `account:DisableRegion`
> - `account:GetRegionOptStatus`
> - `account:ListRegions`

Si utiliza estos permisos individuales, puede conceder a algunos usuarios la capacidad de solo leer la información de opción de región y conceder a otros la capacidad tanto de leer como de escribir.

En el siguiente ejemplo, se habilita una región para la cuenta de miembro especificada en una organización. Las credenciales que se usan deben ser de la cuenta de administración de la organización o de la cuenta de administrador delegado del servicio de Account Management.

Tenga en cuenta que también puede deshabilitar una región con el mismo comando y, a continuación, reemplazar `enable-region` con `disable-region`.

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

Este comando no genera ningún resultado si se utiliza correctamente.

> **Note**
>
> Una organización solo puede tener un máximo de 20 solicitudes de región en un momento dado. De lo contrario, recibirá una `TooManyRequestsException`.

La operación es asíncrona. El siguiente comando le permitirá ver el estado más reciente de la solicitud.

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

Actualiza la facturación de tu Cuenta de AWS

Estas instrucciones muestran cómo actualizar la facturación Cuenta de AWS si te registraste para AWS usar la función de registro AWS (avanzada) o si activaste las funciones avanzadas de tu cuenta. Para comparar las opciones de registro, consultaCompara las opciones de registro.

Puede actualizar todas sus preferencias de Cuenta de AWS facturación mediante la consola AWS Billing de administración de costos. Para obtener información sobre cómo actualizar la configuración relacionada con la facturación de su cuenta, consulte la Guía del usuario de Administración de facturación y costos de AWS:

Actualiza el dirección de correo electrónico del usuario raíz

Estas instrucciones indican cómo actualizar la dirección de correo electrónico del usuario raíz si se ha registrado AWS mediante la opción Registrarse AWS (avanzado) o si ha activado las funciones avanzadas de su cuenta. Para comparar las opciones de registro, consultaCompara las opciones de registro.

Existen varios motivos comerciales por los que es posible que deba actualizar la dirección de correo electrónico del usuario raíz de su Cuenta de AWS. Por ejemplo, la seguridad y la resiliencia administrativa. En este tema se explica el proceso de actualización de la dirección de correo electrónico del usuario raíz, tanto para las cuentas independientes como para las cuentas de miembros.

> **Note**
>
> Los cambios realizados en un Cuenta de AWS anuncio pueden tardar hasta cuatro horas en propagarse por todas partes.

Puede actualizar el correo electrónico del usuario raíz de forma diferente, en función de si las cuentas son independientes o forman parte de una organización:

- Cuentas independientes Cuentas de AWS o de administración: si Cuentas de AWS no están asociadas a una organización, o si son cuentas de administración de una organización, puede actualizar el correo electrónico del usuario raíz, el correo electrónico de mediante la consola AWS de administración. Para obtener información sobre cómo hacerlo, consulte Actualizar el correo electrónico del usuario raíz (correo electrónico de) para una cuenta independiente Cuenta de AWS o de administración.
- Cuentas de AWS dentro de una organización: en el caso de las cuentas de miembros que forman parte de una AWS organización, un usuario de la cuenta de administración o de la cuenta de administrador delegado puede actualizar de forma centralizada el correo electrónico del usuario raíz, el correo de la cuenta del miembro desde la AWS Organizations consola o mediante programación mediante la AWS CLI y los SDK. Para obtener información sobre cómo hacerlo, consulte Actualizar el correo electrónico del usuario raíz de de cualquier parte Cuenta de AWS de su organización.

Temas

- Actualice el correo electrónico del usuario root para una versión independiente Cuenta de AWS o cuenta de administración
- Actualice el correo electrónico del usuario root para cualquier Cuenta de AWS en su organización

Actualice el correo electrónico del usuario root para una versión independiente Cuenta de AWS o cuenta de administración

Para editar la dirección de correo electrónico del usuario raíz, la para una cuenta independiente Cuenta de AWS o de administración, lleve a cabo los pasos del siguiente procedimiento.

Consola de administración de AWS

> **Note**
>
> Debe iniciar sesión como el Usuario raíz de la cuenta de AWS, lo que no requiere permisos de IAM adicionales. No puede realizar estos pasos como usuario o rol de IAM.

1. Usa tu dirección Cuenta de AWS de correo electrónico y contraseña para iniciar sesión en el Consola de administración de AWScomo si fueran tuyas Usuario raíz de la cuenta de AWS.
2. En la esquina superior derecha de la consola, elija el nombre o número de cuenta y, a continuación, seleccione Cuenta.
3. En la página Cuenta, junto a Detalles de la cuenta, seleccione Acciones y, a continuación, seleccione Actualizar dirección de correo electrónico y contraseña.
4. En la página de Detalles de la cuenta, junto a Dirección de correo electrónico, seleccione Editar.
5. En la página Editar correo electrónico, rellene los campos Nueva dirección de correo electrónico, Confirmar la nueva dirección de correo electrónico y confirme su Contraseña actual. A continuación, elija Guardar y continuar. Se envía un código de verificación a la nueva dirección de correo electrónico desde `no-reply@verify.signin.aws`.
6. En la página Editar el correo electrónico de la cuenta, en Código de verificación, introduzca el código que se le envió por correo electrónico y, a continuación, seleccione Confirmar actualizaciones.

> **Note**
>
> El código de verificación puede tardar hasta 5 minutos en llegar. Si no ve el correo en su cuenta, compruebe las carpetas de correo basura y spam.

AWS CLI & SDKs

Esta tarea no es compatible con una operación de API de uno de los AWS SDK AWS CLI ni con ninguna de ellas. Solo puede realizar esta tarea mediante. Consola de administración de AWS

Actualice el correo electrónico del usuario root para cualquier Cuenta de AWS en su organización

Para editar la dirección de correo electrónico del usuario raíz, la para cualquier cuenta de miembro de su organización mediante la AWS Organizations consola, lleve a cabo los pasos del siguiente procedimiento.

> **Note**
>
> Antes de actualizar la dirección de correo electrónico del usuario raíz de una cuenta de miembro, le recomendamos que comprenda el impacto que tiene esta operación. Para obtener más información, consulte Actualización de la dirección de correo electrónico del usuario raíz para una cuenta de miembro con AWS Organizations en la Guía del usuario de AWS Organizations .

También puede actualizar la dirección de correo electrónico del usuario raíz, la de una cuenta de miembro directamente desde la página Cuenta, Consola de administración de AWS después de iniciar sesión como usuario raíz. Para obtener instrucciones paso a paso, siga los pasos que se indican en Actualice el correo electrónico del usuario root para una versión independiente Cuenta de AWS o cuenta de administración.

> **Note**
>
> No puedes actualizar la dirección de correo electrónico del usuario raíz de una cuenta de proyecto, que es una cuenta de miembro que creaste como proyecto en AWS Configuración. Cada cuenta de proyecto es propiedad de un AWS Builder ID, en lugar de la dirección de correo electrónico del usuario raíz, y esto no cambia al activar las funciones avanzadas. Para obtener más información, consulte Proyecte las cuentas después de activar las funciones avanzadas.

AWS Management Console

> **Notas**
>
> - Para llevar a cabo este procedimiento desde la cuenta de administración o desde una cuenta de administrador delegado de una organización y compararla con las cuentas

de miembro, debe habilitar el acceso de confianza al servicio de administración de cuentas.

- No puede utilizar este procedimiento para acceder a una cuenta de una organización diferente a la que utiliza para llamar a la operación.

Para actualizar la dirección de correo electrónico del usuario raíz para una cuenta de miembro que utilice el AWS Organizations consola

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS, elija la cuenta de miembro para la que desee actualizar la dirección de correo electrónico del usuario raíz.
3. En la sección Detalles de la cuenta, seleccione el botón Acciones y, a continuación, seleccione Actualizar dirección de correo electrónico.
4. En Correo electrónico, ingrese la nueva dirección de correo electrónico del usuario raíz y, a continuación, seleccione Guardar. Esto envía una contraseña de un solo uso (OTP) a la nueva dirección de correo electrónico.

   > **Note**
   >
   > Si necesita cerrar esta página en la consola de Organizations mientras espera el código, puede volver y finalizar el proceso de OTP en un plazo de 24 horas a partir del envío del código. Para ello, en la página Detalles de la cuenta, seleccione el botón Acciones y, a continuación, seleccione Completar la actualización del correo electrónico.

5. En Código de verificación, ingrese el código que se envió a la nueva dirección de correo electrónico en el paso anterior y, a continuación, seleccione Confirmar. Esto confirma la actualización en el usuario raíz de la cuenta.

AWS CLI & SDKs

Puede recuperar o actualizar la dirección de correo electrónico del usuario raíz (también denominada dirección de correo electrónico principal) mediante los siguientes AWS CLI comandos o sus operaciones equivalentes al AWS SDK:

- GetPrimaryEmail
- StartPrimaryEmailUpdate
- AcceptPrimaryEmailUpdate

> **Notas**
>
> - Para llevar a cabo estas operaciones desde la cuenta de administración o desde una cuenta de administrador delegado de una organización y compararlas con las cuentas de miembro, debe habilitar el acceso de confianza para el servicio de administración de cuentas.
> - No puedes acceder a una cuenta de una organización diferente a la que utilizas para llamar a la operación.
> - `AcceptPrimaryEmailUpdate`Si se trata de una cuenta `StartPrimaryEmailUpdate` de proyecto, se `AccessDeniedException` produce un error aunque se disponga de los permisos necesarios.

> **Permisos mínimos**
>
> Para cada operación, debe tener el permiso que se asigna a esa operación:
>
> - `account:GetPrimaryEmail`
> - `account:StartPrimaryEmailUpdate`
> - `account:AcceptPrimaryEmailUpdate`
>
> Si utiliza estos permisos individuales, puede conceder a algunos usuarios la capacidad de leer únicamente la información de la dirección de correo electrónico del usuario raíz y conceder a otros la capacidad de leer y escribir.

Para completar el proceso de dirección de correo electrónico del usuario raíz de , debe utilizar las API de correo electrónico principales juntas en el orden en que se muestran en los siguientes ejemplos.

Example **`GetPrimaryEmail`**

En el siguiente ejemplo se recupera la dirección de correo electrónico del usuario raíz de la cuenta de miembro especificada de una organización. Las credenciales utilizadas deben provenir de la cuenta de administración de la organización o de la cuenta de administrador delegado de Account Management.

```
$ aws account get-primary-email --account-id 123456789012
```

Example **`StartPrimaryEmailUpdate`**

En el siguiente ejemplo, se inicia el proceso de actualización de la dirección de correo electrónico del usuario raíz, se identifica la nueva dirección de correo electrónico y se envía una contraseña de un solo uso (OTP) a la nueva dirección de correo electrónico de la cuenta de miembro especificada en una organización. Las credenciales utilizadas deben provenir de la cuenta de administración de la organización o de la cuenta de administrador delegado de Account Management.

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

Example **`AcceptPrimaryEmailUpdate`**

En el siguiente ejemplo, se acepta el código OTP y se establece la nueva dirección de correo electrónico en la cuenta de miembro especificada en una organización. Las credenciales utilizadas deben provenir de la cuenta de administración de la organización o de la cuenta de administrador delegado de la administración de la cuenta.

```
$ aws account accept-primary-email-update --account-id 123456789012 --otp 12345678
 --primary-email john@examplecorp.com
```

Actualizar la contraseña del usuario raíz

Estas instrucciones muestran cómo actualizar la contraseña del usuario raíz si te registraste para AWS usar la opción de registro AWS (avanzada) o si activaste las funciones avanzadas de tu cuenta. Para comparar las opciones de registro, consultaCompara las opciones de registro.

Para editar su contraseña Cuenta de AWS de usuario raíz, siga los pasos del procedimiento siguiente.

Consola de administración de AWS

Para editar la contraseña de su usuario raíz

> **Note**
>
> Debes iniciar sesión como Usuario raíz de la cuenta de AWS, lo que no requiere permisos de IAM adicionales. No puede realizar estos pasos como usuario o rol de IAM.

1. Usa tu dirección Cuenta de AWS de correo electrónico y contraseña para iniciar sesión Consola de administración de AWS como tu Usuario raíz de la cuenta de AWS.
2. En la esquina superior derecha de la consola, elija el nombre o número de cuenta y, a continuación, seleccione Cuenta.
3. En la página Cuenta, junto a Detalles de la cuenta, seleccione Acciones y, a continuación, seleccione Actualizar dirección de correo electrónico y contraseña.
4. En la página de Detalles de la cuenta, junto a Contraseña, seleccione Editar.
5. En la página Editar contraseña, complete los campos Contraseña actual, Contraseña nueva y Confirmar contraseña nueva. A continuación, elija Actualizar contraseña. Para obtener información adicional, incluidas las prácticas recomendadas para configurar las contraseñas de los usuarios raíz, consulte Cambiar la contraseña de la Usuario raíz de la cuenta de AWS en la Guía del usuario de IAM.

AWS CLI & SDKs

Esta tarea no es compatible con ninguna operación de API de uno de los AWS SDK AWS CLI ni con ella. Solo puede realizar esta tarea mediante el Consola de administración de AWS.

Actualiza tu Cuenta de AWS name

Estas instrucciones muestran cómo actualizar tu Cuenta de AWS nombre si te registraste para AWS usar la función de registro AWS (avanzada) o si activaste las funciones avanzadas de tu cuenta. Para comparar las opciones de registro, consultaCompara las opciones de registro.

Cuando administre múltiples unidades Cuentas de AWS, utilice convenciones de nomenclatura claras que coincidan con las unidades de negocio y las aplicaciones para la identificación y la

organización. Durante las reorganizaciones, fusiones, adquisiciones o actualizaciones de las convenciones de nomenclatura, es posible que tenga que cambiar el nombre de las cuentas para mantener estándares administrativos y de identificación uniformes.

El nombre de una cuenta aparece en varios lugares, por ejemplo, en la factura y en consolas, como el panel de control de facturación y gestión de costes y la AWS Organizations consola. Le recomendamos que utilice una forma estándar de asignar nombres a sus cuentas, de modo que los nombres sean fáciles de reconocer. Para cuentas empresariales, considere la posibilidad de utilizar un estándar de nomenclatura, como organización-propósito-entorno (por ejemplo, ventas-catálogo-prod). Por motivos de privacidad y seguridad, evite el uso de nombres de cuenta que reflejen información de identificación personal (PII).

- Cuentas independientes Cuentas de AWS o de administración: en el caso de las cuentas de administración que Cuentas de AWS no estén asociadas a una organización o de la cuenta de administración de una organización, puedes actualizar el nombre de la cuenta mediante los Consola de administración de AWS SDK o AWS CLI los SDK. Para obtener información sobre como hacer esto, consulte Actualiza el nombre de tu cuenta para crear una cuenta independiente Cuenta de AWS o una cuenta de administración.
- Cuentas de AWS dentro de una organización: en el caso de las cuentas de miembros que forman parte de una AWS Organizations, un usuario de la cuenta de administración o de la cuenta de administrador delegado puede actualizar de forma centralizada el nombre de cuenta de cualquier cuenta de miembro de la organización desde la AWS Organizations consola o mediante programación mediante los SDK y. AWS CLI Para obtener información sobre como hacer esto, consulte Actualice el nombre de su cuenta para cualquier Cuenta de AWS en tu organización.

> **Note**
>
> Los cambios en una Cuenta de AWS pueden tardar hasta cuatro horas en propagarse a todas partes.

Temas

- Actualiza el nombre de tu cuenta para crear una cuenta independiente Cuenta de AWS o una cuenta de administración
- Actualice el nombre de su cuenta para cualquier Cuenta de AWS en tu organización

Actualiza el nombre de tu cuenta para crear una cuenta independiente Cuenta de AWS o una cuenta de administración

Para cambiar el nombre de la cuenta de una cuenta independiente Cuenta de AWS o de administración, lleve a cabo los pasos del procedimiento siguiente.

Consola de administración de AWS

> **Permisos mínimos**
>
> Puede actualizar el nombre de cuenta mediante el usuario raíz, un usuario de IAM o un rol de IAM. Si utiliza el usuario raíz, no se necesitan permisos de IAM adicionales para actualizar el nombre de una cuenta. Al utilizar un usuario de IAM o un rol de IAM, debe tener al menos los siguientes permisos de IAM:
>
> - `account:GetAccountInformation`
> - `account:PutAccountName`

Para actualizar el nombre de la cuenta de una cuenta independiente o una cuenta de administración

1. Usa tu dirección Cuenta de AWS de correo electrónico y contraseña para iniciar sesión en ella Consola de administración de AWS como tu Usuario raíz de la cuenta de AWS.
2. En la esquina superior derecha de la consola, elija el nombre o número de cuenta y, a continuación, seleccione Cuenta.
3. En la página Cuenta, junto a Detalles de la cuenta, seleccione Acciones y, a continuación, selecciona Actualizar nombre de cuenta.
4. En Nombre, introduzca el nombre de la nueva cuenta que desea actualizar y, a continuación, seleccione Guardar.

AWS CLI & SDKs

> **Permisos mínimos**
>
> Puede actualizar el nombre de cuenta mediante el usuario raíz, un usuario de IAM o un rol de IAM. Para realizar los siguientes pasos, su usuario de IAM o rol de IAM debe tener al menos los siguientes permisos IAM:

- `account:GetAccountInformation`
- `account:PutAccountName`

Para actualizar el nombre de la cuenta de una cuenta independiente o una cuenta de administración

También puede utilizar una de las siguientes operaciones:

- AWS CLI: put-account-name

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

- AWS SDK: PutAccountName

Actualice el nombre de su cuenta para cualquier Cuenta de AWS en tu organización

En el modo AWS Organizations con todas las funciones, los usuarios de IAM autorizados o los roles de IAM, tanto en las cuentas de administración como en las de administrador delegado, pueden gestionar los nombres de las cuentas de forma centralizada.

Para cambiar el nombre de cuenta para cualquier cuenta de miembro de la organización, siga los pasos que se indican en el siguiente procedimiento.

Requisitos

Para actualizar el nombre de una cuenta con la AWS Organizations consola, debe realizar algunos ajustes preliminares:

- Su organización debe habilitar todas las características para administrar la configuración de las cuentas de sus miembros. Esto le permite al administrador controlar las cuentas de miembro. Esto se establece de forma predeterminada cuando crea la organización. Si su organización está configurada únicamente para la facturación consolidada y desea habilitar todas las características, consulte Habilitación de todas las características para una organización.
- Debe habilitar el acceso confiable para el servicio de administración de AWS cuentas. Para configurarlo, consulte Habilite el acceso confiable para AWS Administración de cuentas.

Consola de administración de AWS

> **Permisos mínimos**
>
> Para actualizar el nombre de una cuenta de miembro, su usuario de IAM o rol de IAM debe tener los siguientes permisos:
>
> - `organizations:DescribeOrganization` (solo consola)
> - `account:PutAccountName`

Para actualizar el nombre de la cuenta de un miembro

1. Abra la consola de organizaciones en https://console.aws.amazon.com/organizations/.
2. En el panel de navegación principal, seleccione Cuentas de AWS.
3. En la página de las Cuentas de AWS, elija la cuenta de miembro que quiere actualizar, seleccione el menú desplegable Acciones y, a continuación, seleccione Actualizar nombre de cuenta.
4. En Nombre, introduzca el nombre actualizado y seleccione Guardar.

AWS CLI & SDKs

> **Permisos mínimos**
>
> Para actualizar el nombre de una cuenta de miembro, su usuario de IAM o rol de IAM debe tener los siguientes permisos:
>
> - `organizations:DescribeOrganization` (solo consola)
> - `account:PutAccountName`

Para actualizar el nombre de la cuenta de un miembro

También puede utilizar una de las siguientes operaciones:

- AWS CLI: put-account-name

```
$ C:\> aws account put-account-name \
```

```
        --account-id 111111111111 \
        --account-name "New-Account-Name"
```

- AWS SDKs: PutAccountName

Actualiza los contactos alternativos de tu Cuenta de AWS

Estas instrucciones muestran cómo actualizar los contactos alternativos de tu cuenta Cuenta de AWS si te registraste para AWS usar la función de registro AWS (avanzada) o si activaste las funciones avanzadas de tu cuenta. Para comparar las opciones de registro, consultaCompara las opciones de registro.

Los contactos alternativos permiten AWS contactar con hasta tres contactos alternativos asociados a la cuenta. El contacto alternativo no tiene que ser una persona específica. En su lugar, puede agregar una lista de distribución de correo electrónico si tiene un equipo que es responsable de administrar los problemas relacionados con la facturación, las operaciones y la seguridad. Estos se suman a la dirección de correo electrónico asociada al usuario raíz de la cuenta. El contacto de la cuenta principal seguirá recibiendo todas las comunicaciones por correo electrónico enviadas al correo electrónico de la cuenta raíz.

Puede especificar solo uno de los siguientes tipos de contacto asociados a una cuenta.

- Contacto de facturación
- Contacto de operaciones
- Contacto de seguridad

Puede agregar o editar contactos alternativos de forma diferente, en función de si las cuentas son independientes o forman parte de una organización:

- Independiente Cuentas de AWS: si Cuentas de AWS no está asociado a una organización, puede actualizar sus propios contactos alternativos mediante la consola de AWS administración o mediante la AWS CLI y los SDK. Para obtener información sobre cómo hacerlo, consulte Actualizar los contactos alternativos para una Cuenta de AWS independiente.
- Cuentas de AWS dentro de una organización: en el caso de las cuentas de miembros que forman parte de una AWS organización, un usuario de la cuenta de administración o de la cuenta de administrador delegado puede actualizar de forma centralizada cualquier cuenta de miembro de la organización desde la AWS Organizations consola o mediante programación mediante la CLI y los

AWS SDK. Para obtener información sobre cómo hacerlo, consulta Cómo actualizar los contactos alternativos de cualquier Cuenta de AWS persona de tu organización.

Temas

- Requisitos de número de teléfono y dirección de correo electrónico
- Actualiza los contactos alternativos para que sean independientes Cuenta de AWS
- Actualiza los contactos alternativos para cualquier Cuenta de AWS en tu organización
- cuenta: clave de AlternateContactTypes contexto

Requisitos de número de teléfono y dirección de correo electrónico

Antes de continuar con la actualización de la información de contactos alternativos de su cuenta, le recomendamos primero revisar los siguientes requisitos cuando ingresa números de teléfono y direcciones de correo electrónico.

- Los números de teléfono solo pueden contener números, espacios en blanco y los siguientes caracteres: "+-( )".
- Las direcciones de correo electrónico pueden tener una longitud máxima de 254 caracteres e incluir los siguientes caracteres especiales en la parte local de la dirección de correo electrónico, además de los caracteres alfanuméricos estándar: "+=.#|!&-_".

Actualiza los contactos alternativos para que sean independientes Cuenta de AWS

Para agregar o editar los contactos alternativos de un contacto independiente Cuenta de AWS, lleve a cabo los pasos del procedimiento siguiente. El Consola de administración de AWS procedimiento siguiente siempre funciona solo en el contexto independiente. Puede utilizarla Consola de administración de AWS para acceder o cambiar únicamente los contactos alternativos de la cuenta que utilizó para llamar a la operación.

Consola de administración de AWS

Para agregar o editar los contactos alternativos de una cuenta independiente Cuenta de AWS

> **Permisos mínimos**
>
> Para realizar los siguientes pasos, debe tener al menos los siguientes permisos IAM:

- `account:GetAlternateContact` (para ver los detalles de contacto alternativos)
- `account:PutAlternateContact` (para configurar o actualizar un contacto alternativo)
- `account:DeleteAlternateContact` (para eliminar un contacto alternativo)

1. Inicie sesión en la Consola de administración de AWS como rol o usuario de IAM con los permisos mínimos.
2. En la parte superior derecha de la ventana, seleccione el nombre de cuenta y, a continuación, seleccione Cuenta.
3. En la página Cuenta, desplácese hacia abajo hasta Contactos alternativos y, a la derecha del título, seleccione Editar.

> **Note**
>
> Si no ves la opción Editar, es probable que no hayas iniciado sesión como usuario raíz de tu cuenta o como alguien que tenga los permisos mínimos especificados anteriormente.

4. Cambie los valores de cualquiera de los campos disponibles.

> **Important**
>
> En el caso de las empresas Cuentas de AWS, se recomienda introducir el número de teléfono y la dirección de correo electrónico de la empresa en lugar de los de una persona.

5. Luego de realizar todos los cambios, elija Hecho.

AWS CLI & SDKs

Puedes recuperar, actualizar o eliminar la información de contacto alternativa mediante los siguientes AWS CLI comandos o sus operaciones equivalentes en el AWS SDK:

- GetAlternateContact
- PutAlternateContact
- DeleteAlternateContact

> **Notas**
>
> - Para realizar estas operaciones desde la cuenta de administración o desde una cuenta de administrador delegado de una organización y compararlas con las cuentas de los miembros, debe habilitar el acceso de confianza al servicio de Cuenta.

> **Permisos mínimos**
>
> Para cada operación, debe tener el permiso que se asigna a esa operación:
>
> - `GetAlternateContact` (para ver los detalles de contacto alternativos)
> - `PutAlternateContact` (para configurar o actualizar un contacto alternativo)
> - `DeleteAlternateContact` (para eliminar un contacto alternativo)
>
> Si utiliza estos permisos individuales, puede conceder a algunos usuarios la capacidad de leer únicamente la información de contacto y conceder a otros la capacidad de leer y escribir.

Example

En el siguiente ejemplo, se recupera el contacto alternativo de facturación actual de la cuenta de la persona que llama.

```
$ 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

En el siguiente ejemplo, se establece un nuevo contacto alternativo de Operaciones para la cuenta de la persona que llama.

```
$ 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"
```

Este comando no genera ningún resultado si se utiliza correctamente.

Example

> **Note**
>
> Si realizas varias `PutAlternateContact` operaciones en el mismo Cuenta de AWS tipo de contacto, la primera agrega el nuevo contacto y todas las llamadas sucesivas al mismo Cuenta de AWS tipo de contacto actualizan el contacto existente.

Example

En el siguiente ejemplo, se elimina el contacto alternativo de seguridad de la cuenta de la persona que llama.

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

Este comando no genera ningún resultado si se utiliza correctamente.

> **Note**
>
> Si intenta eliminar el mismo contacto más de una vez, el primero lo hará de forma silenciosa. Todos los intentos posteriores generan una excepción `ResourceNotFound`.

Actualiza los contactos alternativos para cualquier Cuenta de AWS en tu organización

Para agregar o editar los detalles de contacto alternativos de cualquier Cuenta de AWS miembro de su organización, siga los pasos del procedimiento siguiente.

Requisitos

Para actualizar los contactos alternativos con la AWS Organizations consola, debe realizar algunos ajustes preliminares:

- Su organización debe habilitar todas las características para administrar la configuración de las cuentas de sus miembros. Esto le permite al administrador controlar las cuentas de miembro. Esto se establece de forma predeterminada cuando crea la organización. Si su organización está configurada únicamente para la facturación consolidada y desea habilitar todas las características, consulte Habilitación de todas las características para una organización.
- Debe habilitar el acceso confiable para el servicio de administración de AWS cuentas. Para configurarlo, consulte Habilite el acceso confiable para AWS Administración de cuentas.

> **Note**
>
> Las políticas AWS Organizations administradas `AWSOrganizationsReadOnlyAccess` o `AWSOrganizationsFullAccess` se actualizan para permitir el acceso a las API de administración de AWS cuentas, de modo que puedas acceder a los datos de la cuenta desde la AWS Organizations consola. Para ver las políticas administradas actualizadas, consulta Actualizaciones de las políticas AWS administradas de las organizaciones.

Consola de administración de AWS

Para agregar o editar los contactos alternativos de cualquier Cuenta de AWS en su organización

1. Inicie sesión en la consola de AWS Organizations con las credenciales de la cuenta de administración de la organización.
2. En Cuentas de AWS, seleccione la cuenta que desea actualizar.
3. Seleccione Información de contacto y, en Contactos alternativos, busque el tipo de contacto: contacto de facturación, contacto de seguridad o contacto de operaciones.
4. Para agregar un contacto nuevo, seleccione Agregar o, para actualizar un contacto existente, seleccione Editar.
5. Cambie los valores de cualquiera de los campos disponibles.

> **Important**
>
> En el caso de las empresas Cuentas de AWS, se recomienda introducir el número de teléfono y la dirección de correo electrónico de la empresa en lugar de los que pertenezcan a una persona.

6. Luego de realizar todos los cambios, elija Hecho.

AWS CLI & SDKs

Puedes recuperar, actualizar o eliminar la información de contacto alternativa mediante los siguientes AWS CLI comandos o sus operaciones equivalentes en el AWS SDK:

- GetAlternateContact
- PutAlternateContact
- DeleteAlternateContact

> **Notas**
>
> - Para realizar estas operaciones desde la cuenta de administración o desde una cuenta de administrador delegado de una organización y compararlas con las cuentas de los miembros, debe habilitar el acceso de confianza al servicio de Cuenta.

- No puedes acceder a una cuenta de una organización diferente a la que estás usando para llamar a la operación.

Permisos mínimos

Para cada operación, debe tener el permiso que se asigna a esa operación:

- `GetAlternateContact` (para ver los detalles de contacto alternativos)
- `PutAlternateContact` (para configurar o actualizar un contacto alternativo)
- `DeleteAlternateContact` (para eliminar un contacto alternativo)

Si utiliza estos permisos individuales, puede conceder a algunos usuarios la capacidad de leer únicamente la información de contacto y conceder a otros la capacidad de leer y escribir.

Example

En el siguiente ejemplo, se recupera el contacto alternativo de facturación actual de la cuenta de la persona que llama en una organización. Las credenciales utilizadas deben provenir de la cuenta de administración de la organización o de la cuenta de administrador delegado de Account Management.

```
$ 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

En el siguiente ejemplo, se establece el contacto alternativo de operaciones para la cuenta de miembro especificada en una organización. Las credenciales utilizadas deben provenir de la cuenta de administración de la organización o de la cuenta de administrador delegado de Account Management.

```
$ 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"
```

Este comando no genera ningún resultado si se utiliza correctamente.

> **Note**
>
> Si realizas varias `PutAlternateContact` operaciones en el mismo Cuenta de AWS tipo de contacto, la primera agrega el nuevo contacto y todas las llamadas sucesivas al mismo Cuenta de AWS tipo de contacto actualizan el contacto existente.

Example

En el siguiente ejemplo, se elimina el contacto alternativo de seguridad de la cuenta de miembro especificada en una organización. Las credenciales utilizadas deben provenir de la cuenta de administración de la organización o de la cuenta de administrador delegado de Account Management.

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

Este comando no genera ningún resultado si se utiliza correctamente.

Example

> **Note**
>
> Si intenta eliminar el mismo contacto más de una vez, el primero lo hará de forma silenciosa. Todos los intentos posteriores generan una excepción `ResourceNotFound`.

cuenta: clave de AlternateContactTypes contexto

Puede usar la clave de contexto `account:AlternateContactTypes` para especificar cuál de los tres tipos de contacto está permitido (o denegado) según la política de IAM. Por ejemplo, en el siguiente ejemplo, la política de permisos de IAM utiliza esta clave de condición para permitir que las entidades principales adjuntas recuperen, pero no modifiquen, únicamente el contacto alternativo `BILLING` de una cuenta específica de una organización.

Como `account:AlternateContactTypes` es un tipo de cadena con varios valores, debe utilizar los operadores de cadena con varios valores `ForAnyValue o ForAllValues`.

Actualiza el contacto principal de tu Cuenta de AWS

Estas instrucciones indican cómo actualizar tu contacto principal Cuenta de AWS si te has registrado AWS con la opción Registrarse AWS (avanzado) o si has activado las funciones avanzadas de tu cuenta. Para comparar las opciones de registro, consultaCompara las opciones de registro.

Puede actualizar la información de contacto principal asociada a su cuenta, incluidos su nombre completo de contacto, nombre de empresa, dirección postal, número de teléfono y dirección de sitio web.

También puedes verificar el número de teléfono de contacto principal. Para obtener más información, consulte Verifica el número de teléfono de contacto principal.

Puede editar el contacto de cuenta primaria de forma diferente, en función de si las cuentas son independientes o no parte de una organización:

- Independiente Cuentas de AWS: si Cuentas de AWS no está asociado a una organización, puede actualizar el contacto de su cuenta principal mediante la consola AWS de administración o mediante AWS CLI y SDK. Para obtener información sobre cómo hacerlo, consulte Actualizar el contacto principal independiente. Cuenta de AWS

- Cuentas de AWS dentro de una organización: en el caso de las cuentas de miembros que forman parte de una AWS organización, un usuario de la cuenta de administración o de la cuenta de administrador delegado puede actualizar de forma centralizada cualquier cuenta de miembro de la organización desde la AWS Organizations consola o mediante programación mediante la AWS CLI y los SDK. Para obtener información sobre cómo hacerlo, consulta Actualizar el contacto Cuenta de AWS principal de tu organización.

Temas

- Requisitos de número de teléfono y dirección de correo electrónico
- Actualiza el contacto principal para convertirlo en un contacto independiente Cuenta de AWS o cuenta de administración
- Actualiza el contacto principal de cualquier AWS cuenta de miembro de su organización
- Verifica el número de teléfono de contacto principal

Requisitos de número de teléfono y dirección de correo electrónico

Antes de continuar con la actualización de la información de contacto principal de su cuenta, le recomendamos revisar los siguientes requisitos al ingresar números de teléfono y direcciones de correo electrónico.

- Los números de teléfono solo deben contener números.
- Los números de teléfono deben comenzar con un + y un código de país no deben tener ceros a la izquierda ni espacios adicionales después del código de país. Por ejemplo, +1 (US/Canada) o +44 (UK).
- Los números de teléfono no deben incluir espacios en blanco entre el código de área, el código de cambio y el código local. Por ejemplo, +12025550179.
- Por motivos de seguridad, los números de teléfono deben poder recibir SMS desde AWS. No se aceptarán números gratuitos, ya que la mayoría no admiten SMS.
- En el caso de las empresas Cuentas de AWS, se recomienda introducir el número de teléfono y la dirección de correo electrónico de la empresa en lugar de los de una persona física. Configurar el usuario raíz de la cuenta con la dirección de correo electrónico o el número de teléfono de una persona puede dificultar la recuperación de la cuenta si esa persona deja la empresa.

Actualiza el contacto principal para convertirlo en un contacto independiente Cuenta de AWS o cuenta de administración

Para editar sus datos de contacto principales para una cuenta independiente Cuenta de AWS o de administración, lleve a cabo los pasos del siguiente procedimiento. El siguiente Consola de administración de AWS procedimiento siempre funciona solo en el contexto independiente. Puede utilizar la Consola de administración de AWS para acceder o cambiar únicamente la información de contacto principal de la cuenta que utilizó para llamar a la operación.

Consola de administración de AWS

Para editar su contacto principal para convertirlo en un contacto independiente Cuenta de AWS o cuenta de administración

> **Permisos mínimos**
>
> Para realizar los siguientes pasos, debe tener al menos los siguientes permisos IAM:
>
> - `account:GetContactInformation` (para ver los detalles de contacto principales)
> - `account:PutContactInformation` (para actualizar los detalles de contacto principales)

1. Inicie sesión en la Consola de administración de AWS como rol o usuario de IAM con los permisos mínimos.
2. En la parte superior derecha de la ventana, seleccione el nombre de cuenta y, a continuación, seleccione Cuenta.
3. Desplácese hacia abajo hasta la sección Información de contacto y, junto a ella, seleccione Editar.
4. Cambie los valores de cualquiera de los campos disponibles.
5. Luego de realizar todos los cambios, elija Hecho.

AWS CLI & SDKs

Puedes recuperar, actualizar o eliminar la información de contacto principal mediante los siguientes AWS CLI comandos o sus operaciones equivalentes al AWS SDK:

- GetContactInformation
- PutContactInformation

> **Notas**
>
> - Para realizar estas operaciones desde la cuenta de administración o desde una cuenta de administrador delegado de una organización y compararlas con las cuentas de los miembros, debe habilitar el acceso de confianza al servicio de Cuenta.

> **Permisos mínimos**
>
> Para cada operación, debe tener el permiso que se asigna a esa operación:
>
> - `account:GetContactInformation`
> - `account:PutContactInformation`
>
> Si utiliza estos permisos individuales, puede conceder a algunos usuarios la capacidad de leer únicamente la información de contacto y conceder a otros la capacidad de leer y escribir.

Example

En el siguiente ejemplo, se recupera la información de contacto principal actual de la cuenta de la persona que llama.

```
$ 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

En el siguiente ejemplo, se establece la nueva información de contacto principal para la cuenta de la persona que llama.

```
$ 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"}'
```

Este comando no genera ningún resultado si se utiliza correctamente.

Actualiza el contacto principal de cualquier AWS cuenta de miembro de su organización

Para editar sus datos de contacto principales en cualquier cuenta de AWS miembro de su organización, lleve a cabo los pasos del siguiente procedimiento.

Requisitos adicionales

Para actualizar el contacto principal con la AWS Organizations consola, debe realizar algunos ajustes preliminares:

- Su organización debe habilitar todas las características para administrar la configuración de las cuentas de sus miembros. Esto le permite al administrador controlar las cuentas de miembro. Esto se establece de forma predeterminada cuando crea la organización. Si su organización está configurada únicamente para la facturación consolidada y desea habilitar todas las características, consulte Habilitación de todas las características para una organización.
- Debes habilitar el acceso confiable al servicio de administración de AWS cuentas. Para configurarlo, consulte Habilite el acceso confiable para AWS Administración de cuentas.

Consola de administración de AWS

Para editar tu contacto principal para cualquier Cuenta de AWS en tu organización

1. Inicie sesión en la consola de AWS Organizations con las credenciales de la cuenta de administración de la organización.
2. En Cuentas de AWS, seleccione la cuenta que desea actualizar.
3. Selecciona Información de contacto y localiza el contacto principal.
4. Seleccione Editar.
5. Cambie los valores de cualquiera de los campos disponibles.
6. Una vez que hayas realizado todos los cambios, selecciona Guardar.

Si cambias el número de teléfono, te enviaremos un código de verificación al nuevo número cuando selecciones Guardar. Puedes verificar el número inmediatamente o más tarde. Para obtener más información, consulte Verifica el número de teléfono de una cuenta de miembro de tu organización.

AWS CLI & SDKs

Puedes recuperar, actualizar o eliminar la información de contacto principal mediante los siguientes AWS CLI comandos o sus operaciones equivalentes al AWS SDK:

- GetContactInformation
- PutContactInformation

> **Notas**
>
> - Para realizar estas operaciones desde la cuenta de administración o desde una cuenta de administrador delegado de una organización y compararlas con las cuentas de los miembros, debe habilitar el acceso de confianza al servicio de Cuenta.
> - No puedes acceder a una cuenta de una organización diferente a la que utilizas para llamar a la operación.

Permisos mínimos

Para cada operación, debe tener el permiso que se asigna a esa operación:

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

Si utiliza estos permisos individuales, puede conceder a algunos usuarios la capacidad de leer únicamente la información de contacto y conceder a otros la capacidad de leer y escribir.

Example

En el siguiente ejemplo, se recupera la información de contacto principal actual para la cuenta de miembro especificada en una organización. Las credenciales utilizadas deben provenir de la cuenta de administración de la organización o de la cuenta de administrador delegado de Account Management.

```
$ 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

En el siguiente ejemplo, se establece la información de contacto principal para la cuenta de miembro especificada en una organización. Las credenciales utilizadas deben provenir de la

cuenta de administración de la organización o de la cuenta de administrador delegado de Account Management.

```
$ 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"}'
```

Este comando no genera ningún resultado si se utiliza correctamente.

Verifica el número de teléfono de contacto principal

Puede verificar el número de teléfono en la información de contacto principal de un Cuenta de AWS. La verificación confirma que el número de teléfono registrado puede recibir nuestros mensajes de texto SMS.

Al iniciar la verificación, enviamos un código de verificación de 6 dígitos por mensaje de texto SMS al número de teléfono registrado actualmente en la cuenta. No introduzcas un número de teléfono para iniciar la verificación. Para terminar, debes introducir el código antes de que caduque.

Ten en cuenta lo siguiente cuando verifiques un número de teléfono:

- El código caduca 5 minutos después de que lo enviemos.
- Si solicitas un código nuevo, los códigos que te enviamos anteriormente ya no funcionan.
- Si el código es incorrecto o ha caducado, solicita un código nuevo e inténtalo de nuevo.
- Si el número de teléfono cambia después de que te enviemos un código, no podrás usarlo. Solicita un código nuevo para el número actual.
- El estado de verificación siempre describe el número de teléfono que está registrado actualmente. Si cambias el número de teléfono, el estado describe el nuevo número.
- En el caso de una cuenta de miembro de una organización, el código va al número de teléfono de contacto principal de la cuenta de miembro, no al tuyo. Antes de empezar, asegúrate de poder obtener el código de la persona que tenga ese teléfono.

Para comprobar el estado de la verificación, utilice la GetContactInformationoperación. El `VerificationStatus` campo de la respuesta tiene uno de los siguientes valores:

- `VERIFIED`— El número de teléfono registrado está verificado.
- `UNVERIFIED`— El número de teléfono registrado no está verificado.
- `NOT_SUPPORTED`— La verificación del número de teléfono no está disponible para esta cuenta.

Verifica el número de teléfono de una empresa independiente o de administración Cuenta de AWS

Para verificar el número de teléfono de la cuenta cuyas credenciales utilizas, usa los siguientes AWS CLI comandos o sus operaciones equivalentes al AWS SDK:

- SendPhoneNumberVerification
- VerifyPhoneNumber

> **Permisos mínimos**
>
> Para cada operación, debe tener el permiso que se asigna a esa operación:
>
> - `account:SendPhoneNumberVerification`
> - `account:VerifyPhoneNumber`
>
> Para comprobar el estado de la verificación, también necesitas`account:GetContactInformation`.

Example

El siguiente AWS CLI ejemplo envía un código de verificación al número de teléfono de contacto principal de la cuenta de la persona que llama:

```
$ aws account send-phone-number-verification
{
    "Status": "PENDING"
}
```

Example

En el siguiente AWS CLI ejemplo, se envía el código para finalizar la verificación:

```
$ aws account verify-phone-number --otp 123456
```

```
{
    "Status": "VERIFIED"
}
```

Example

El siguiente AWS CLI ejemplo recupera el estado de verificación del número de teléfono de contacto principal de la persona que llama:

```
$ aws account get-contact-information --query VerificationStatus
"VERIFIED"
```

Verifica el número de teléfono de una cuenta de miembro de tu organización

Puede verificar el número de teléfono de una cuenta de miembro mediante la AWS Organizations consola AWS CLI, el o un AWS SDK. Antes de empezar, complete los pasos que se indican a continuaciónRequisitos adicionales.

Consola de administración de AWS

Para verificar el número de teléfono de contacto principal de una cuenta de miembro

> **Permisos mínimos**
>
> Para realizar los siguientes pasos, debe tener al menos los siguientes permisos IAM:
>
> - `account:GetContactInformation`(para ver el número de teléfono y si está verificado)
> - `account:SendPhoneNumberVerification`(para enviar un código de verificación)
> - `account:VerifyPhoneNumber`(para enviar el código)
>
> La política `AWSOrganizationsFullAccess` gestionada no incluye `account:SendPhoneNumberVerification` o`account:VerifyPhoneNumber`. Si se basa en esa política, conceda estos permisos por separado.

1. Inicie sesión en la consola de AWS Organizations con las credenciales de la cuenta de administración de la organización.
2. Desde Cuentas de AWS, selecciona la cuenta del miembro.

3. Elija Información de contacto y localice el contacto principal.
4. Si el número de teléfono no está verificado, aparecerá con una advertencia. Elige el número de teléfono y, a continuación, selecciona Verificar número de teléfono. Enviamos un código de 6 dígitos al número de teléfono de la cuenta del miembro.
5. Introduce el código en Código de verificación y, a continuación, selecciona Verificar.

   Si el código no llega, selecciona Reenviar el código cuando la opción esté disponible.

AWS CLI & SDKs

Para verificar el número de teléfono de la cuenta de un miembro, usa los siguientes AWS CLI comandos o sus operaciones equivalentes al AWS SDK y especifica el ID de la cuenta del miembro:

- SendPhoneNumberVerification
- VerifyPhoneNumber

> **Notas**
>
> - Las credenciales que utilices deben provenir de la cuenta de administración de la organización o de la cuenta de administrador delegado para la administración de AWS cuentas.
> - No puedes acceder a una cuenta de una organización diferente a la que utilizas para llamar a la operación.

> **Permisos mínimos**
>
> Para cada operación, debe tener el permiso que se asigna a esa operación:
>
> - `account:SendPhoneNumberVerification`
> - `account:VerifyPhoneNumber`
>
> Para comprobar el estado de la verificación, también necesitas`account:GetContactInformation`.

Example

El siguiente AWS CLI ejemplo envía un código de verificación al número de teléfono de contacto principal de la cuenta de miembro especificada:

```
$ aws account send-phone-number-verification --account-id 123456789012
{
    "Status": "PENDING"
}
```

Example

El siguiente AWS CLI ejemplo envía el código que enviamos al número de teléfono de la cuenta del miembro:

```
$ aws account verify-phone-number --account-id 123456789012 --otp 123456
{
    "Status": "VERIFIED"
}
```

Visualización Cuenta de AWS identificadores

Esta información trata sobre la visualización de Cuenta de AWS los identificadores si te has registrado para AWS usar la función de registro AWS (avanzada) o si has activado las funciones avanzadas de tu cuenta. Para comparar las opciones de registro, consulta. Compara las opciones de registro

AWS asigna los siguientes identificadores únicos a cada uno: Cuenta de AWS

Cuenta de AWS ID

Un número de 12 dígitos, por ejemplo 012345678901, que identifica de forma única una Cuenta de AWS. Muchos AWS recursos incluyen el identificador de la cuenta en sus nombres de recursos de Amazon (ARN). La parte de ID de cuenta diferencia los recursos en una cuenta de los recursos en otra. Si es un usuario AWS Identity and Access Management (IAM), puede iniciar sesión Consola de administración de AWS con el ID de la cuenta o el alias de la cuenta. Si bien los ID de cuenta, al igual que cualquier información de identificación, deben usarse y compartirse con cuidado, no se consideran información secreta, sensible o confidencial.

ID de usuario canónico

Un identificador alfanumérico, por ejemplo `79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be`, que es una forma ofuscada del ID. Cuenta de AWS Puede usar este ID para identificar y Cuenta de AWS cuando conceda acceso multicuenta a depósitos y objetos mediante Amazon Simple Storage Service (Amazon S3). Puede recuperar el ID de usuario canónico de la Cuenta de AWS como el usuario raíz o un usuario de IAM.

Debes estar autenticado con AWS para ver estos identificadores.

> **Warning**
>
> No proporciones tus AWS credenciales (incluidas las contraseñas y las claves de acceso) a un tercero que necesite tus Cuenta de AWS identificadores para compartir AWS recursos contigo. Hacerlo les daría el mismo acceso Cuenta de AWS que tú tienes.

Encuentra tu Cuenta de AWS ID

Puedes encontrar el Cuenta de AWS ID usando el Consola de administración de AWS o el AWS Command Line Interface (AWS CLI). En la consola, la ubicación del ID de la cuenta depende de si has iniciado sesión como usuario raíz o como usuario de IAM. El ID de la cuenta es el mismo tanto si ha iniciado sesión como usuario raíz como usuario de IAM.

Encontrar el ID de cuenta como el usuario raíz

Consola de administración de AWS

Para encontrar tu Cuenta de AWS ID al iniciar sesión como usuario raíz

> **Permisos mínimos**
>
> Para realizar los siguientes pasos, debe tener al menos los siguientes permisos IAM:
>
> - Cuando inicia sesión como usuario raíz, no necesita permisos de IAM.

1. En la barra de navegación de la parte superior derecha, elija el nombre o número de la cuenta y, a continuación, seleccione Credenciales de seguridad.

> **Tip**
>
> Si no ve la opción Credenciales de seguridad, es posible que haya iniciado sesión como usuario federado con un rol de IAM, en lugar de como usuario de IAM. En este caso, busque la entrada Cuenta y el número de ID de cuenta que aparece junto a ella.

2. En la sección Detalles de la cuenta, el número de cuenta aparece junto al ID de la Cuenta de AWS .

AWS CLI & SDKs

Para encontrar tu Cuenta de AWS ID, usa el AWS CLI

> **Permisos mínimos**
>
> Para realizar los siguientes pasos, debe tener al menos los siguientes permisos IAM:
>
> - Cuando ejecuta el comando como usuario raíz, no necesita permisos de IAM.

Use el comando get-caller-identity de la siguiente manera.

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

Encontrar el ID de cuenta como un usuario de IAM

Consola de administración de AWS

Para encontrar su Cuenta de AWS ID al iniciar sesión como usuario de IAM

> **Permisos mínimos**
>
> Para realizar los siguientes pasos, debe tener al menos los siguientes permisos IAM:

- `account:GetAccountInformation`

1. En la barra de navegación de la parte superior derecha, elija el nombre de usuario y, a continuación, seleccione Credenciales de seguridad.

   > **Tip**
   >
   > Si no ve la opción Credenciales de seguridad, es posible que haya iniciado sesión como usuario federado con un rol de IAM, en lugar de como usuario de IAM. En este caso, busque la entrada Cuenta y el número de ID de cuenta que aparece junto a ella.

2. En la parte superior de la página, en Detalles de la cuenta, el número de cuenta aparece junto al ID de Cuenta de AWS .

AWS CLI & SDKs

Para encontrar su Cuenta de AWS ID, utilice el AWS CLI

> **Permisos mínimos**
>
> Para realizar los siguientes pasos, debe tener al menos los siguientes permisos IAM:
>
> - Cuando ejecuta el comando como rol o usuario de IAM, debe tener:
>   - `sts:GetCallerIdentity`

Use el comando get-caller-identity de la siguiente manera.

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

Busca el seudónimo canónico de tu Cuenta de AWS

Puedes encontrar el seudónimo canónico para Cuenta de AWS usar el o el. Consola de administración de AWS AWS CLI El seudónimo canónico de un Cuenta de AWS es específico de esa cuenta. Puedes recuperar tu ID de usuario canónico Cuenta de AWS como usuario raíz, usuario federado o usuario de IAM.

Encontrar el ID canónico como usuario raíz o usuario de IAM

Consola de administración de AWS

Cómo encontrar el ID de usuario canónico de su cuenta cuando ha iniciado sesión en la consola como usuario raíz o usuario de IAM

> **Permisos mínimos**
>
> Para realizar los siguientes pasos, debe tener al menos los siguientes permisos IAM:
>
> - Cuando ejecuta el comando como usuario raíz, no necesita permisos de IAM.
> - Cuando inicia sesión como usuario de IAM, debe tener:
>   - `account:GetAccountInformation`

1. Inicia sesión como usuario raíz o Consola de administración de AWS como usuario de IAM.
2. En la barra de navegación de la parte superior derecha, elija el nombre o número de la cuenta y, a continuación, seleccione Credenciales de seguridad.

   > **Tip**
   >
   > Si no ve la opción Credenciales de seguridad, es posible que haya iniciado sesión como usuario federado con un rol de IAM, en lugar de como usuario de IAM. En este caso, busque la entrada Cuenta y el número de ID de cuenta que aparece junto a ella.

3. En la sección Detalles de la cuenta, el ID de usuario canónico aparece junto al ID de usuario canónico. Puede usar su ID de usuario canónico para configurar las listas de control de acceso (ACL) de Amazon S3.

AWS CLI & SDKs

Para buscar el ID de usuario canónico, utilice el AWS CLI

El mismo comando AWS CLI y el de la API funcionan para los Usuario raíz de la cuenta de AWS usuarios de IAM o los roles de IAM.

Use el comando list-buckets de la siguiente manera.

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

Encontrar el ID canónico como usuario federado con un rol de IAM

Consola de administración de AWS

Cómo encontrar el ID canónico de su cuenta cuando ha iniciado sesión en la consola como usuario federado con un rol de IAM

> **Permisos mínimos**
>
> - Debe tener permiso para enumerar y ver un bucket de Amazon S3.

1. Inicie sesión Consola de administración de AWS como usuario federado con un rol de IAM.
2. En la consola de Amazon S3, elija un nombre de bucket para ver los detalles de un bucket.
3. Elija la pestaña Permisos.
4. En la sección Lista de control de acceso, en Propietario del bucket, aparece el ID canónico de su Cuenta de AWS .

AWS CLI & SDKs

Para buscar el ID de usuario canónico, utilice el AWS CLI

El mismo comando AWS CLI y el de la API funcionan para los Usuario raíz de la cuenta de AWS usuarios de IAM o los roles de IAM.

Use el comando list-buckets de la siguiente manera.

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

Solucione sus problemas Cuenta de AWS

Esta información trata sobre la solución de problemas Cuenta de AWS si te has registrado para AWS usar la función de registro AWS (avanzada) o si has activado las funciones avanzadas de tu cuenta. Para comparar las opciones de registro, consultaCompara las opciones de registro.

Utilice la información compartida en los siguientes temas para diagnosticar y solucionar problemas con su Cuenta de AWS. Para obtener ayuda con el usuario raíz, consulte Solución de problemas con el usuario raíz en la Guía del usuario de IAM. Para obtener ayuda con el proceso de inicio de sesión, consulte Solución de problemas de inicio de Cuenta de AWS sesión en la Guía del AWS Sign-In usuario.

Temas de solución de problemas

- Solución de problemas con Cuenta de AWS creación
- Solución de problemas con Cuenta de AWS cierre
- Solución de otros problemas con Cuentas de AWS

Solución de problemas con Cuenta de AWS creación

Esta información trata sobre la solución de problemas relacionados con Cuenta de AWS la creación si te has registrado para AWS usar la función de registro AWS (avanzada) o si has activado las funciones avanzadas de tu cuenta. Para comparar las opciones de registro, consultaCompara las opciones de registro.

Utilice los enlaces de referencia de la tabla siguiente para diagnosticar y solucionar los problemas relacionados con la creación de una nueva Cuenta de AWS.

Problema	Enlace de referencia	origen
No sé cómo registrarme o crear una cuenta	Registrarse en AWS (avanzado)	Esta guía
¿Qué debo hacer si no he recibido una llamada AWS para verificar mi nueva cuenta o si el PIN que he introducido no funciona?	https://repost.aws/knowledge-center/phone-verify-no-call	AWS re:Post
¿Cómo soluciono el error del «número máximo de intentos fallidos» cuando intento verificar mi identidad Cuenta de AWS por teléfono?	https://repost.aws/knowledge-center/maximum-failed-attempts	AWS re:Post
Han pasado más de 24 horas y mi cuenta no está activada	https://repost.aws/knowledge-center/create-and-activate-aws-account	AWS re:Post
No puedo iniciar sesión en mi nueva cuenta después de haberla creado	https://docs.aws.amazon.com/signin/latest/userguide/troubleshooting-sign-in-issues.html	AWS Sign-In Guía del usuario

Para obtener ayuda adicional, le recomendamos que busque AWS re:Post a fin de obtener contenido relacionado con su problema específico. Si necesita ayuda, póngase en contacto con AWS Support.

Solución de problemas con Cuenta de AWS cierre

Esta información trata sobre la solución de problemas relacionados con el Cuenta de AWS cierre si te has registrado para AWS usar la función de registro AWS (avanzada) o si has activado las funciones avanzadas de tu cuenta. Para comparar las opciones de registro, consultaCompara las opciones de registro.

Utilice la información que se indica a continuación para diagnosticar y solucionar los problemas comunes que puedan surgir durante el proceso de cierre de la cuenta. Para obtener información general sobre el proceso de cierre de cuentas, consulte Cerrar un Cuenta de AWS.

Temas

- No sé cómo eliminar o cancelar mi cuenta
- No veo el botón Cerrar cuenta en la página de la cuenta
- He cerrado mi cuenta, pero aún no he recibido una confirmación por correo electrónico
- Recibo el error ConstraintViolationException «» al intentar cerrar mi cuenta
- Recibo el mensaje de error "CLOSE_ACCOUNT_QUOTA_EXCEEDED" cuando intento cerrar una cuenta de miembro
- ¿Tengo que eliminar mi AWS ¿La organización antes de cerrar la cuenta de administración?

No sé cómo eliminar o cancelar mi cuenta

Para cerrar su cuenta, siga las instrucciones de Cerrar un Cuenta de AWS.

No veo el botón Cerrar cuenta en la página de la cuenta

Si no ha iniciado sesión como usuario raíz, no verá el botón Cerrar cuenta en la página de la cuenta. Debe iniciar sesión Consola de administración de AWS como usuario root para cerrar su cuenta. Si no puede iniciar sesión, consulte Solucionar problemas con el usuario raíz.

He cerrado mi cuenta, pero aún no he recibido una confirmación por correo electrónico

Este correo electrónico de confirmación solo se envía a la dirección de correo electrónico del usuario raíz de la para la Cuenta de AWS. Si no recibes este correo electrónico en unas horas, puedes iniciar sesión Consola de administración de AWS como usuario raíz para comprobar que tu cuenta está cerrada. Si su cuenta se ha cerrado correctamente, aparecerá un mensaje que indica que su cuenta está cerrada. Si la cuenta que has cerrado es una cuenta de miembro, puedes comprobar si la cuenta cerrada se ha cerrado correctamente si la cuenta cerrada está etiquetada como `CLOSED` en la AWS Organizations consola. Para obtener más información, consulte Cierre de una cuenta miembro de la organización en la Guía del usuario de AWS Organizations .

Si está intentando cerrar una cuenta de administración y no recibe un correo electrónico de confirmación sobre el cierre de la cuenta, lo más probable es que su organización tenga cuentas de miembro activas. Solo puede cerrar la cuenta de administración si su organización no tiene ninguna cuenta de miembro activa. Para comprobar que no quedan cuentas de miembros activas en tu organización, ve a la AWS Organizations consola y asegúrate de que todas las cuentas de los miembros aparezcan `Closed` junto a sus nombres de cuenta. Después de eso, puede cerrar la cuenta de administración.

Recibo el error ConstraintViolationException «» al intentar cerrar mi cuenta

Estás intentando cerrar una cuenta de administración desde la AWS Organizations consola, pero no es posible. Para cerrar una cuenta de administración, debe iniciar sesión Consola de administración de AWS como usuario raíz de la cuenta de administración y cerrarla desde la página de cuentas. Para obtener más información, consulte Closing a management account in your organization en la Guía del usuario de AWS Organizations .

Recibo el mensaje de error "CLOSE_ACCOUNT_QUOTA_EXCEEDED" cuando intento cerrar una cuenta de miembro

Solo puedes cerrar el 20% de las cuentas de los miembros en un período continuo de 30 días. Esta cuota no está vinculada a un mes natural, sino que comienza cuando se cierra una cuenta. Dentro de los 30 días posteriores al cierre inicial de la cuenta, no puedes superar el límite de cierre de la cuenta del 20%. El cierre mínimo de la cuenta es de 250 y el cierre máximo de la cuenta es de 1000, incluso si el 20% de las cuentas supera los 1000. Para obtener más información sobre las cuotas de Organizations, consulte Quotas for AWS Organizations en la Guía del usuario de AWS Organizations .

¿Tengo que eliminar mi AWS ¿La organización antes de cerrar la cuenta de administración?

No, no es necesario que elimines tu AWS organización antes de cerrar la cuenta de administración. Sin embargo, solo puede cerrar la cuenta de administración si su organización no tiene ninguna cuenta de miembro activa. Para comprobar que no quedan cuentas de miembros activas en tu organización, ve a la AWS Organizations consola y asegúrate de que todas las cuentas de los miembros aparezcan `Closed` junto a sus nombres de cuenta. Después de eso, puede cerrar la cuenta de administración.

Solución de otros problemas con Cuentas de AWS

Esta información trata sobre cómo solucionar otros problemas Cuenta de AWS si te registraste para AWS usar Registrarse AWS (avanzado) o si activaste las funciones avanzadas de tu cuenta. Para comparar las opciones de registro, consultaCompara las opciones de registro.

Utilice la información que aquí se incluye para solucionar problemas relacionados con su Cuenta de AWS.

Problemas

- Necesito cambiar la tarjeta de crédito de mi Cuenta de AWS
- Necesito denunciar un caso fraudulento Cuenta de AWS activity
- Necesito cerrar mi Cuenta de AWS
- Recibo una AccessDeniedExceptioncuando actualizo la dirección de correo electrónico de un usuario root

Necesito cambiar la tarjeta de crédito de mi Cuenta de AWS

Para cambiar tu tarjeta de crédito Cuenta de AWS, debes poder iniciar sesión. AWS cuenta con protecciones que requieren que demuestres que eres el propietario de la cuenta. Para obtener instrucciones, consulte Managing your credit card payment methods en la Guía del usuario de AWS Billing .

Necesito denunciar un caso fraudulento Cuenta de AWS activity

Si sospechas que se ha realizado un uso fraudulento de tus recursos Cuenta de AWS y quieres denunciarlos, consulta Cómo denuncio el uso indebido de AWS recursos.

Si tienes problemas con una compra realizada en Amazon.com, consulta el Servicio de atención al cliente de Amazon.

Necesito cerrar mi Cuenta de AWS

Si necesitas ayuda para solucionar problemas relacionados con el cierre de tu Cuenta de AWS, consultaCerrar un Cuenta de AWS.

Recibo una **`AccessDeniedException`**cuando actualizo la dirección de correo electrónico de un usuario root

Si la cuenta del miembro es una cuenta de proyecto, no puedes actualizar la dirección de correo electrónico del usuario raíz. Cada cuenta de proyecto es propiedad de un AWS Builder ID, en lugar de la dirección de correo electrónico del usuario raíz. Para obtener más información, consulte Proyecte las cuentas después de activar las funciones avanzadas.

Administre las cuentas en India

Esta información se refiere a la administración de cuentas en India si te registraste para AWS usar Registrarse AWS (avanzado) o si activaste funciones avanzadas para tu cuenta. Para comparar las opciones de registro, consultaCompara las opciones de registro.

Si te registras en una nueva dirección Cuenta de AWS y eliges India como dirección de contacto y facturación, tu acuerdo de usuario se celebra con Amazon Web Services India Private Limited (AWS India), un AWS vendedor local en la India. AWS India gestiona la facturación y el total de la factura se indica en rupias indias (INR) en lugar de en dólares estadounidenses (USD). Para obtener información sobre la gestión de una Cuenta de AWS, consulte. Configura tu Cuenta de AWS

Si su cuenta está en AWS India, siga los procedimientos de este tema para administrarla. En este tema se explica cómo abrir una cuenta en AWS India, editar la información sobre tu cuenta en AWS India, gestionar la verificación de clientes y añadir o editar tu número de cuenta permanente (PAN).

Como parte de la verificación de la tarjeta de crédito durante el registro, AWS India carga 2 INR a tu tarjeta de crédito. AWS India reembolsa los 2 INR una vez realizada la verificación. Es posible que se le redirija a su banco como parte del proceso de verificación.

Temas

- Crea un Cuenta de AWS por AWS India
- Administre la información de verificación del cliente

Crea un Cuenta de AWS por AWS India

AWS India es un vendedor local AWS de India. Si su dirección de contacto y facturación se encuentra en la India y desea crear una cuenta, utilice el siguiente procedimiento para crear una cuenta en AWS la India.

Para suscribirse a una AWS Cuenta en India

1. Abra la página de inicio de Amazon Web Services.
2. Elige Crear un Cuenta de AWS.

> **Note**
>
> Si has iniciado sesión AWS recientemente, es posible que esa opción no esté disponible. En su lugar, elija Iniciar sesión en la consola. Si la opción Crear una Cuenta de AWS nueva no está visible, seleccione Iniciar sesión en otra cuenta y, a continuación, seleccione Crear una Cuenta de AWS nueva.

3. Introduzca la información de su cuenta, verifique su dirección de correo electrónico y elija una contraseña segura para su cuenta.

4. Elija Empresarial o Personal. Las cuentas personales y las cuentas empresariales tienen las mismas características y funciones.
5. Introduzca la información de su empresa o su información de contacto personal. Si su dirección de contacto o facturación se encuentra en la India, de conformidad con las normas del Equipo de Respuesta a Emergencias Informáticas de la India (CERT-In), AWS debe recopilar y validar su información de identidad antes de concederle acceso a AWS los servicios.

   El nombre que elijas entre tu información de contacto o de facturación debe coincidir exactamente con el nombre que aparece en el documento que piensas usar para la verificación del cliente. Por ejemplo, si planea verificar una cuenta empresarial mediante un certificado de constitución, debe proporcionar el nombre comercial que aparece en el documento. Para obtener una lista de los tipos de documentos aceptados, consulte the section called “Documentos de la India aceptados para la verificación del cliente”.
6. Después de leer el acuerdo del cliente, seleccione la casilla de verificación de términos y condiciones y, a continuación, elija Continuar.
7. En la página Información de facturación, especifique el medio de pago que desee utilizar. Debe proporcionar su CVV como parte del proceso de verificación.
8. En ¿Tiene un PAN? , elija Sí si tiene un número de cuenta permanente (PAN) que le gustaría que apareciera en sus facturas de impuestos y, a continuación, introduzca su PAN. Si no tiene un PAN o quiere agregarlo después de registrarse, seleccione No.
9. Selecciona Verificar y continuar. AWS India carga 2 INR a tu tarjeta como parte del proceso de verificación. AWS India reembolsa los 2 INR una vez realizada la verificación.
10. En la página Confirmar su identidad, seleccione el propósito principal del registro de la cuenta.
11. Elija el tipo de propiedad que mejor representa al propietario de la cuenta. Si elige una empresa, organización o asociación como el tipo de propiedad, ingrese el nombre del contacto administrativo clave. El contacto administrativo clave puede ser un director, un jefe de operaciones o una persona a cargo de las operaciones de su empresa.
12. En función del tipo de propiedad que haya seleccionado, elija un documento aceptado de la India para utilizarlo en la verificación e ingrese su información de documento.

> **Note**
>
> Si tiene una cuenta personal y planea usar un permiso de conducir no emitido por la Unión de la India, le recomendamos que utilice un tipo de documento personal diferente para la verificación.

13. Seleccione el nombre que desea utilizar para la verificación del cliente.

    Los nombres de su información de contacto y facturación aparecerán para que los seleccione si están asociados a una dirección de la India. Asegúrese de que el nombre elegido coincide con el nombre del tipo de documento que piensa usar para la verificación del cliente. Si necesita modificar el nombre asociado a su dirección de contacto o facturación, puede hacerlo una vez completado el registro de la cuenta.

14. Autorice el envío de su información a efectos de verificación y, a continuación, seleccione Continuar.

    Recibirá una notificación por correo electrónico sobre el resultado de la verificación del cliente después de completar el inicio de sesión de la cuenta. También puedes comprobar el estado en la página de verificación del cliente en la configuración de tu cuenta o en el AWS Health Dashboard más adelante. Para acceder a los servicios de AWS , debe pasar la verificación del cliente.

15. Para verificar su número de teléfono móvil, seleccione Mensaje de texto (SMS) o Llamada de voz.

16. Elija su código de país o región e ingrese su número de teléfono.

17. Complete el control de seguridad.

18. Elija Enviar SMS o Llámame ahora. Momentos después, recibirá un PIN de cuatro dígitos en un SMS o en una llamada automática en su teléfono móvil.

19. En la página Confirme su identidad, introduzca el PIN que recibió y seleccione Continuar.

20. En la página Seleccione un plan de soporte, elija la opción que desee y, a continuación, Completar registro. Una vez verificados tu método de pago y la verificación del cliente, se activará tu cuenta y recibirás un correo electrónico confirmando la activación de la misma.

> **Note**
>
> Si completó la verificación de cliente y modificó el nombre, la dirección o el tipo de documento utilizado anteriormente para verificar su identidad, es posible que tenga que volver a pasar la verificación. Para obtener más información, consulte the section called “Edite la información de verificación del cliente”.

Administre la información de verificación del cliente

De conformidad con las normas del Equipo de Respuesta a Emergencias Informáticas de la India (CERT-In), AWS está obligado a recopilar y validar su información de identidad antes de concederle un acceso nuevo o continuo a AWS los servicios. Para verificar su identidad, deberá utilizar el nombre de la dirección de contacto o facturación de la India que haya facilitado. Durante la verificación, AWS comprobará si el número de documento es válido y si el nombre que has proporcionado coincide con el nombre asociado al documento que utilizas para la verificación del cliente. El nombre de su información de contacto o de facturación debe coincidir con el nombre que aparece en el documento.

Para actualizar su nombre y dirección de facturación, consulte la página de preferencias de pago. Para actualizar su nombre y dirección de contacto, consulte the section called “Actualiza el contacto principal de tu Cuenta de AWS”. Si editas cualquier información que hayas utilizado anteriormente para la verificación del cliente, como el nombre o la India-based dirección de tu información de facturación o de contacto, es posible que tengas que actualizar y volver a enviar tu información de verificación de cliente.

Compruebe el estado de verificación del cliente

Puede ver el estado de verificación del cliente en cualquier momento en la página Verificación del cliente. Si el estado de verificación indica Verificación obligatoria o Verificación errónea, cree o actualice la información de verificación del cliente y envíela de nuevo para su posterior verificación.

Si tu cuenta de administración ha habilitado la herencia de verificaciones de clientes, el estado de verificación de tu cuenta refleja el estado de esa cuenta. No es necesario que realices ninguna acción cuando la herencia esté activa.

Cree la información de verificación del cliente

Para completar la verificación como cliente, tendrá que proporcionar la información de un documento aceptado en la India. Para obtener una lista de los tipos de documentos aceptados, consulte the section called “Documentos de la India aceptados para la verificación del cliente”.

1. Inicie sesión en el Consola de administración de AWS.
2. En la barra de navegación situada en la esquina superior derecha, elija su nombre de cuenta (o alias) y, a continuación, elija Mi cuenta.
3. En Otros ajustes, elija Verificación del cliente.

Si aún no ha proporcionado su información de verificación de cliente, verá la página Crear una verificación de cliente.

4. Elija el nombre que coincide exacto con el nombre del documento que piensa usar para la verificación del cliente. Por ejemplo, si planea verificar una cuenta empresarial mediante un certificado de constitución, debe proporcionar el nombre comercial que aparece en el documento.
5. Proporcione el resto de la información solicitada en la página. Según el tipo de documento que elija, es posible que tenga que cargar una copia tanto del anverso como del reverso del documento. Si sube un archivo de imagen, asegúrese de que toda la información del documento esté visible y sea legible.
6. Seleccione Enviar.

   Se le notificará el resultado de la verificación del cliente y cualquier paso siguiente por correo electrónico o en el AWS Health Dashboard.

Edite la información de verificación del cliente

Puede editar la información de verificación de sus clientes, como el propósito principal del registro de la cuenta, el tipo de organización y el nombre, el tipo de documento, la carga del documento o la información del documento que desea usar para la verificación.

Si edita el nombre o el tipo de documento para utilizarlos en la verificación del cliente, o si actualiza la información de algún documento, deberá volver a verificar su identidad al guardar los cambios.

> **La herencia de verificación está activa**
>
> Si su cuenta de administración ha habilitado la herencia de verificaciones de clientes, no podrá editar ni enviar su propia información de verificación de clientes. La información de verificación aparece en modo de solo lectura.

1. Inicie sesión en el Consola de administración de AWS.
2. En la barra de navegación situada en la esquina superior derecha, elija su nombre de cuenta (o alias) y, a continuación, elija Mi cuenta.
3. En Otros ajustes, elija Verificación del cliente.
4. Elija Editar y, a continuación, actualice la información que desea cambiar.

A medida que actualice la información, tenga en cuenta las siguientes instrucciones:

- Si elige un nombre diferente, el nombre debe coincidir exacto con el nombre del documento que piensa usar para la verificación del cliente. Por ejemplo, si planea verificar una cuenta empresarial mediante un certificado de constitución, debe proporcionar el nombre comercial que aparece en el documento.
- Si elige un tipo de documento diferente, tendrá que cargar una copia del anverso y el reverso (si corresponde) del documento. Toda la información de la carga del documento debe ser visible y legible.
- Si tiene una cuenta personal y planea usar un permiso de conducir no emitido por la Unión de la India, le recomendamos que utilice un tipo de documento personal diferente para la verificación.

  Para obtener una lista de los tipos de documentos aceptados, consulte the section called “Documentos de la India aceptados para la verificación del cliente”.

5. Seleccione Enviar.

   Si es necesario volver a verificar su identidad debido al tipo de cambios que ha guardado, se le notificará el resultado de la verificación por parte del cliente y los pasos a seguir por correo electrónico. También puede ver los resultados volviendo a la página de verificación del cliente o al AWS Health Dashboard.

Gestione la herencia de verificaciones del cliente para AWS Organizations

Con AWS Organizations, puede habilitar la herencia de verificaciones de clientes para su organización. Cuando habilitas la herencia, las cuentas de India-based los miembros de tu organización heredan el estado de verificación de tu cuenta de administración. No necesitan completar la verificación del cliente de forma independiente.

Su cuenta de administración debe completar su propia verificación de cliente antes de poder habilitar la herencia. Una vez habilitada la herencia, no es necesario que vuelva a enviar los documentos de verificación.

Cuando tu cuenta de administración habilita la herencia de la verificación por parte del cliente, el estado de verificación se extiende a las cuentas de India-based los miembros de tu organización. En el caso de esas cuentas de miembros, es posible que usemos o divulguemos tu información de verificación en respuesta a solicitudes de las autoridades o de las autoridades reguladoras.

Activa o desactiva la herencia de verificaciones de los clientes

Utilice el siguiente procedimiento para activar o desactivar la herencia de verificaciones de clientes en las cuentas de India-based los miembros de su organización.

1. Abre el Consola de administración de AWS chat Consola de administración de AWS.
2. En la barra de navegación, elige el nombre de tu cuenta (o alias) y, a continuación, selecciona Cuenta.
3. En Otros ajustes, elija Verificación del cliente.
4. En la configuración de verificación del cliente, activa la opción Herencia para activar la herencia o desactívala para desactivarla.
5. Revise el cuadro de diálogo de confirmación y, a continuación, confirme su elección.

Cuando habilitas la herencia, todas las cuentas de los India-based miembros de tu organización heredan tu estado de verificación. Al inhabilitar la herencia, restablecemos el estado de verificación previa de las cuentas de los miembros que previamente completaron su propia verificación. Una cuenta de miembro sin verificación previa debe completar la verificación del cliente de forma independiente.

Verificación de cliente para AWS Cuentas de miembros de Organizations

Si tu cuenta tiene una dirección de India-based contacto o de facturación, heredas el estado de verificación de la cuenta de administración. Esto se aplica cuando tu cuenta de administración ha habilitado la herencia de la verificación del cliente. Puedes ver un mensaje en la página de verificación del cliente que lo confirma.

Cuando la herencia está activa, no puedes enviar ni editar tu propia información de verificación de cliente. No es necesario que realice ninguna acción.

Si su cuenta de administración inhabilita la herencia, debe tener su propio estado de verificación de cliente. Lo mismo se aplica si tu cuenta abandona la organización o si la cuenta de administración elimina tu cuenta de la organización. Si anteriormente enviaste tu propia información de verificación, restablecemos tu estado de verificación anterior. No necesitas repetir el proceso. Esta restauración solo se aplica si su nombre y dirección no han cambiado desde la última verificación.

Documentos de la India aceptados para la verificación del cliente

Para la verificación del cliente, se aceptan los siguientes tipos de documentos expedidos por el gobierno de la India.

> **Note**
>
> Los siguientes enlaces están sujetos a cambios por parte del gobierno.

- Tarjeta PAN: disponible en formato digital y físico, la tarjeta de número de cuenta permanente (PAN) contiene un identificador alfanumérico único expedido por el Departamento de Impuestos sobre la Renta de la India a personas físicas, empresas y entidades. Un PAN consta de diez caracteres, incluidos letras y números, con el formato **`AAAAA1111A`**. Para usar este documento como verificación, también debe proporcionar la fecha de nacimiento (persona física) o la fecha de constitución (empresa) que aparece en el documento PAN y cargar la parte frontal de la tarjeta. Para comprobar la validez de su PAN, consulte el sitio web oficial del Departamento de Impuestos sobre la Renta.
- Identificación de elector Card/EPIC: la tarjeta de identificación de votante, también conocida como tarjeta de identidad con fotografía del elector (EPIC), contiene un número de identificación único emitido por la Comisión Electoral de la India a los votantes elegibles en la India. El ID/EPIC número de elector consta de diez caracteres, que incluyen letras y números. Puede visitar el sitio web oficial de la Comisión Electoral de la India para comprobar la validez de su identificación de votante. Para usar este documento para la verificación, debe cargar tanto el anverso como el reverso de la tarjeta.
- Licencia de conducir: si su licencia de conducir no ha sido emitida por la Unión de la India, le recomendamos que utilice un tipo de documento diferente para la verificación. Un número de licencia de conducir consta de entre 12 y 16 caracteres, incluidos letras, números, espacios y guiones. Para usar este documento para la verificación, debe proporcionar la fecha de nacimiento y cargar tanto el anverso como el reverso de la tarjeta. Para comprobar la validez de su licencia de conducir, consulte el sitio web Parivahan Sewa del Ministerio de Transporte y Vialidad.
- Certificado de constitución: un certificado de constitución es un documento emitido por el Ministerio de Asuntos Corporativos (MCA) que fecha el registro de una empresa como entidad legal. El certificado se utiliza para identificar y localizar de manera exclusiva a las empresas registradas en la India. Cada certificado contiene un número de identificación corporativa (CIN), que es un identificador alfanumérico único que consta de 21 caracteres, incluidos letras y números. Para utilizar este documento para la verificación, debe cargar el documento del certificado de constitución. Puede ir al portal del Ministerio de Asuntos Corporativos para comprobar la validez de su CIN.

Se aceptan distintos tipos de documentos de la India para la apertura de cuentas personales y empresariales:

- Para cuentas personales: carné PAN, carné de votante y carné de conducir. card/EPIC
- Para cuentas comerciales: tarjeta PAN y certificado de constitución.

Administre sus AWS Cuenta en India

A excepción de las siguientes tareas, los procedimientos para administrar su cuenta son los mismos que los de las cuentas creadas fuera de la India. Para obtener información general sobre la administración de su cuenta, consulte the section called “Configure su cuenta”.

Consola de administración de AWS Utilícela para realizar las siguientes tareas:

- Agregar o editar un número de cuenta permanente
- Editar varios números de cuenta permanente
- the section called “Administre la información de verificación del cliente”
- Editar varios números de impuestos de bienes y servicios (GST)
- Ver una factura fiscal

Cerrar un Cuenta de AWS

Estas instrucciones indican cómo cerrar tu cuenta Cuenta de AWS si te has registrado para AWS usar Registrarse AWS (avanzado) o si has activado las funciones avanzadas de tu cuenta. Para comparar las opciones de registro, consultaCompara las opciones de registro.

Si ya no la necesitas Cuenta de AWS, puedes cerrarla en cualquier momento siguiendo las instrucciones de esta sección. Una vez que la haya cerrado, podrá volver a abrirla en un plazo de 90 días a partir del día en que la cerró. El período comprendido entre el día en que se cerró la cuenta y el momento en que se cierra AWS definitivamente la cuenta se denomina período posterior al cierre.

Qué debe saber antes de cerrar su cuenta

Antes de cerrar la suya Cuenta de AWS, debe tener en cuenta lo siguiente:

- El cierre de su cuenta servirá como aviso de rescisión del Acuerdo del cliente de AWS de esta cuenta.

- No es necesario que elimine los recursos de su cuenta Cuenta de AWS antes de cerrarla. Sin embargo, le recomendamos que haga una copia de seguridad de los recursos o datos que desee conservar. Para obtener instrucciones sobre cómo hacer una copia de seguridad de un recurso concreto, consulte la documentación de AWS correspondiente a ese servicio.
- Puede volver a abrir su cuenta durante el periodo posterior al cierre. Los cargos por los servicios que permanecieron en su cuenta se reiniciarán si la vuelve a abrir. También sigue siendo responsable de las facturas impagas, de las Instancias reservadas y los Savings Plans pendientes.
- Usted sigue siendo responsable de todas las tarifas y los cargos pendientes por los servicios utilizados antes del cierre de la cuenta. Recibirás una AWS factura al mes siguiente de cerrar tu cuenta. Por ejemplo, si cerró su cuenta el 15 de enero, recibirá una factura a principios de febrero por el uso realizado entre el 1 y el 15 de enero. Seguirá recibiendo las facturas de Instancias reservadas y Savings Plans después de cerrar su cuenta hasta que venzan.
- Ya no podrás acceder a los AWS servicios que antes estaban disponibles en tu cuenta. Sin embargo, puedes iniciar sesión y acceder a una cuenta cerrada Cuenta de AWS durante el período posterior al cierre solo para ver la información de facturación anterior, acceder a la configuración de la cuenta o ponerte en contacto con AWS Supportella.
- No podrá utilizar la misma dirección de correo electrónico con la que estaba registrado en su Cuenta de AWS en el momento del cierre como el correo electrónico principal de otra Cuenta de AWS. Si desea utilizar la misma dirección de correo electrónico para una Cuenta de AWS diferente, le recomendamos que la actualice antes del cierre. Para obtener más información, consulte Actualiza el dirección de correo electrónico del usuario raíz.
- No puedes usar el mismo alias de cuenta que registraste Cuenta de AWS en el momento del cierre para otra Cuenta de AWS. Para volver a utilizar el alias para otro Cuenta de AWS, elimina el alias de la cuenta antes de cerrarla. Para obtener más información, consulta Cómo usar un alias para tu Cuenta de AWS ID en la Guía del usuario de IAM.
- Si ha activado la autenticación multifactor (MFA) en el usuario raíz de Cuenta de AWS o ha configurado un dispositivo MFA en un usuario de IAM, la MFA no se elimina automáticamente cuando se cierra la cuenta. Si decide dejar MFA activada durante el periodo de 90 días posterior al cierre, mantenga activo el dispositivo MFA hasta que haya caducado el periodo posterior al cierre, por si necesita acceder a la cuenta durante ese tiempo. Tenga en cuenta que los dispositivos con token TOTP de equipo no se pueden asociar a otro usuario luego del cierre permanente de su cuenta. Si desea utilizar el token TOTP de equipo con otro usuario más adelante, tiene la opción de desactivar el dispositivo MFA de equipo antes de cerrar la cuenta. Los dispositivos MFA para usuarios de IAM debe eliminarlos el administrador de la cuenta.

Consideraciones adicionales para las cuentas de miembro

- Cuando cierra una cuenta de miembro, esa cuenta no se elimina de la organización hasta después de transcurrido el periodo posterior al cierre. Durante el periodo posterior al cierre, una cuenta de miembro cerrada aún genera costos en la cuota de las cuentas de la organización. Para evitar que la cuenta se contabilice para la cuota, consulte Remove a member account from your organization antes de cerrarla.
- Solo puede cerrar el 20% o 250 de las cuentas de los miembros hasta un máximo de 1000 en un período continuo de 30 días, lo que sea mayor. Esta cuota no está vinculada a un mes natural, sino que comienza cuando se cierra una cuenta. Para obtener más información sobre las cuotas de Organizations, consulte Quotas for AWS Organizations.
- Si utilizas AWS Control Tower, tendrás que dejar de administrar la cuenta de miembro antes de intentar cerrarla. Consulte Anular la administración de una cuenta de miembro en la Guía del usuario de AWS Control Tower.

Consideraciones específicas del servicio

- AWS Marketplace las suscripciones no se cancelan automáticamente al cerrar la cuenta. Si tiene alguna suscripción, primero cancele todas las instancias del software incluidas en las suscripciones. A continuación, vaya a la página Administrar suscripciones de la AWS Marketplace consola y cancele las suscripciones.
- Tras cerrar una cuenta, AWS enviaremos correos electrónicos diarios durante un máximo de cinco días antes de que suspendamos el dominio. Una vez suspendido el dominio, y en función del registrador del dominio, eliminaremos el dominio en un plazo de 30 días o entregaremos el dominio a su registrador. Para obtener más información, consulte Mi dominio Cuenta de AWS está cerrado o cerrado permanentemente y mi dominio está registrado en Route 53.

  Si la dirección de correo electrónico del usuario raíz de esta cuenta usa un dominio registrado a través de Route 53 en la misma cuenta, no cierre la cuenta hasta que complete una de las siguientes acciones: transferir el dominio a otro Cuenta de AWS o actualizar la dirección de correo electrónico del usuario raíz para usar un dominio que no esté registrado en esta cuenta. De lo contrario, al cerrar la cuenta se suspende el dominio, lo que interrumpe la entrega de correo electrónico a su dirección de usuario raíz. Sin correo electrónico, no puedes recuperar la cuenta y, sin ella, no puedes restablecer el dominio. Transcurridos 30 días, Route 53 elimina el dominio de forma permanente. Esto también se aplica a las cuentas de los miembros cuyas direcciones de correo electrónico de usuario raíz utilizan dominios registrados en esta cuenta.

- AWS CloudTrail es un servicio de seguridad fundamental. Esto significa que las rutas creadas por los usuarios pueden seguir existiendo y publicando eventos incluso después de que una Cuenta de AWS esté cerrada, a menos que un usuario elimine explícitamente las rutas de las suyas Cuenta de AWS antes de cerrarla. Para obtener más información sobre cómo solicitar la eliminación de una ruta después de haber Cuenta de AWS sido cerrada, consulta la sección sobre el Cuenta de AWS cierre y las rutas en la Guía del CloudTrail usuario.

Cómo cerrar su cuenta

Puede cerrar el suyo Cuenta de AWS mediante el siguiente procedimiento. Tenga en cuenta que hay diferentes instrucciones en cada pestaña según el tipo de cuenta [independiente, de miembro, de administración y AWS GovCloud (US)] que desee cerrar.

Si tiene algún problema durante el proceso de cierre de su cuenta, consulte Solución de problemas con Cuenta de AWS cierre.

Standalone account

Una cuenta independiente es una cuenta gestionada de forma individual que no forma parte de ella. AWS Organizations

Cómo cerrar una cuenta independiente desde la página de la cuenta

1. Inicie sesión Consola de administración de AWS como usuario raíz en la Cuenta de AWS que desee cerrar. Si inicia sesión como un rol o usuario de IAM, no puede cerrar una cuenta.
2. En la barra de navegación situada en la esquina superior derecha, elija el nombre o número de cuenta y, a continuación, elija Cuenta.
3. En la página de la cuenta, seleccione el botón Cerrar cuenta.
4. Escriba su ID de cuenta (que aparece en la parte superior del cuadro de diálogo de cierre) para confirmar que ha leído y comprendido el proceso de cierre de la cuenta.
5. Pulse el botón Cerrar cuenta para iniciar el proceso de cierre de cuenta.
6. En unos minutos, recibirá un correo electrónico de confirmación de que su cuenta se ha cerrado.

> **Note**
>
> Esta tarea no es compatible con una operación de API de uno de los AWS SDK AWS CLI ni con ninguna de ellas. Solo puede realizar esta tarea mediante. Consola de administración de AWS

Member account

Una cuenta de miembro es una Cuenta de AWS que forma parte de AWS Organizations.

Para cerrar una cuenta de miembro desde AWS Organizations consola

1. Inicie sesión en la consola de AWS Organizations.
2. En la página Cuentas de AWS, busque y elija el nombre de la cuenta de miembro que desea cerrar. Puede navegar por la jerarquía de unidades organizativas o ver una lista plana de cuentas sin la estructura de unidad organizativa.
3. Selecciona Cerrar cuenta junto al nombre de la cuenta en la parte superior de la página. Esta opción solo está disponible cuando una organización de AWS está en el modo Todas las características.

   > **Note**
   >
   > Si su organización utiliza el modo de facturación unificada, no podrá ver el botón Cerrar cuenta en la consola. Para cerrar una cuenta en el modo de Facturación unificada, inicie sesión en la cuenta que desee cerrar como usuario raíz. En la página Cuentas, pulse el botón Cerrar cuenta, ingrese el ID de su cuenta y, a continuación, pulse el botón Cerrar cuenta.

4. Lea y asegúrese de comprender la guía para el cierre de la cuenta.
5. Introduzca el ID de cuenta de miembro y, a continuación, elija Cerrar cuenta para iniciar el proceso de cierre de cuenta.

> **Note**
>
> Cualquier cuenta de miembro que cierre mostrará una etiqueta `CLOSED` junto al nombre de la cuenta en la consola de AWS Organizations hasta 90 días después de la fecha de

cierre original. Transcurridos 90 días, la cuenta de miembro dejará de mostrarse en la consola de AWS Organizations .

Para cerrar una cuenta de miembro desde la página Cuentas

Si lo desea, puede cerrar la cuenta de un AWS miembro directamente desde la página Cuenta del Consola de administración de AWS. Para obtener instrucciones paso a paso, sigue las instrucciones que aparecen en la pestaña Cuenta independiente.

Esta opción no está disponible para las cuentas de proyectos que no tienen un usuario root. Cierra las cuentas del proyecto desde la AWS Organizations consola.

Para cerrar una cuenta de miembro mediante AWS CLI un SDK

Para obtener instrucciones sobre cómo cerrar una cuenta de miembro mediante los SDK AWS CLI y, consulte Cerrar una cuenta de miembro en su organización en la Guía del AWS Organizations usuario.

Management account

Una cuenta de administración es Cuenta de AWS aquella que actúa como cuenta principal o raíz de AWS Organizations.

> **Note**
>
> No puede cerrar una cuenta de administración directamente desde la consola de AWS Organizations .

Cómo cerrar una cuenta de administración desde la página de la cuenta

1. Inicie sesión Consola de administración de AWS como usuario raíz de la cuenta de administración que desee cerrar. Si inicia sesión como un rol o usuario de IAM, no puede cerrar una cuenta.
2. Compruebe que no queden cuentas de miembro activas en su organización. Para ello, vaya a la consola de AWS Organizations y asegúrese de que todas las cuentas de miembro tengan la etiqueta `Closed` junto a sus nombres de cuenta. Si tiene una cuenta de miembro que sigue activa, tendrá que seguir las instrucciones para cerrar la cuenta que se proporcionan en la pestaña Cuenta de miembro antes de pasar al siguiente paso.

3. En la barra de navegación situada en la esquina superior derecha, elija el nombre o número de cuenta y, a continuación, elija Cuenta.
4. En la página de la cuenta, seleccione el botón Cerrar cuenta.
5. Escriba su ID de cuenta (que aparece en la parte superior del cuadro de diálogo de cierre) para confirmar que ha leído y comprendido el proceso de cierre de la cuenta.
6. Pulse el botón Cerrar cuenta para iniciar el proceso de cierre de cuenta.
7. En unos minutos, recibirá un correo electrónico de confirmación de que su cuenta se ha cerrado.

> **Note**
>
> Esta tarea no es compatible con ninguna operación de API de uno de los AWS SDK. AWS CLI Solo puede realizar esta tarea mediante. Consola de administración de AWS

AWS GovCloud (US) account

Una AWS GovCloud (US) cuenta siempre está vinculada a un único estándar Cuenta de AWS para fines de facturación y pago.

Para cerrar una AWS GovCloud (US) cuenta

Si tienes una Cuenta de AWS que está vinculada a una AWS GovCloud (US) cuenta, debes cerrar la cuenta estándar antes de cerrar la AWS GovCloud (US) cuenta. Para obtener más información, incluida la forma de hacer copias de seguridad de los datos y evitar AWS GovCloud (US) cargos imprevistos, consulta Cómo cerrar una AWS GovCloud (US) cuenta en la Guía del AWS GovCloud (US) usuario.

Qué esperar después de cerrar su cuenta

Inmediatamente después de cerrar la cuenta, ocurrirá lo siguiente:

- Recibirá un correo electrónico en la dirección de correo electrónico del usuario raíz con la confirmación del cierre de la cuenta. Si no recibe este correo electrónico en unas horas, consulte Solución de problemas con Cuenta de AWS cierre.
- Cualquier cuenta de miembro que cierres mostrará una `CLOSED` etiqueta junto al nombre de la cuenta en la AWS Organizations consola hasta 90 días después de la fecha de cierre original.

Transcurridos 90 días, la cuenta de miembro dejará de mostrarse en la AWS Organizations consola.

- Si has concedido permisos de acceso a los servicios de tu cuenta Cuenta de AWS a otras cuentas, cualquier solicitud de acceso realizada desde esas cuentas debería fallar tras el cierre de la cuenta. Si vuelves a abrir la tuya Cuenta de AWS, otras Cuentas de AWS personas podrán volver a acceder a AWS los servicios y recursos de tu cuenta si les has concedido los permisos necesarios.

Es posible que el cierre de la cuenta no se produzca de inmediato en todas las regiones y servicios, y puede tardar varias horas en completarse.

Post-closure punto

El período posterior al cierre se refiere al tiempo transcurrido entre el día en que cerró su cuenta y el momento en que la cierra AWS permanentemente. Cuenta de AWS El periodo posterior al cierre es de 90 días. Durante el periodo posterior al cierre, solo puede acceder al contenido y los servicios de AWS si reabre la cuenta. Tras el periodo posterior al cierre, cierra la tuya Cuenta de AWS de AWS forma permanente y ya no podrás volver a abrirla. AWS también eliminará el contenido y los recursos de tu cuenta (excepto las CloudTrail rutas). Una vez que una cuenta se haya cerrado permanentemente, su ID de Cuenta de AWS no se podrá volver a utilizar.

Reabrir tu Cuenta de AWS

Tu cuenta se cerrará permanentemente en 90 días. Transcurridos estos 90 días, no podrás volver a abrirla y AWS eliminarás el contenido restante de la misma. Para volver a abrir su cuenta antes de que se cierre definitivamente, consulte. Vuelva a abrir un Cuenta de AWS

> **Note**
>
> Los cargos por los servicios que permanecieron en su cuenta se reiniciarán si la vuelve a abrir.

Vuelva a abrir un Cuenta de AWS

Si has cerrado tu cuenta Cuenta de AWS y no tienes saldo pendiente, puedes volver a abrirla tú mismo durante el período posterior al cierre.

Para volver a abrir la cuenta, inicie sesión como usuario root y envíe la solicitud desde la página de cuentas.

Lo que debes saber antes de volver a abrir tu cuenta

Antes de volver a abrir la suya Cuenta de AWS, tenga en cuenta lo siguiente:

- Self-service requisitos: Puede utilizar este proceso de autoservicio solo si ha cerrado la cuenta usted mismo y si ésta no tenía saldo pendiente en el momento del cierre de la cuenta. Debes iniciar sesión como usuario raíz de la cuenta cerrada; no puedes volver a abrir una cuenta si has iniciado sesión como usuario o rol de IAM. Debes enviar tu solicitud de reapertura en un plazo de 90 días a partir del cierre de la cuenta, durante el período posterior al cierre.
- Cuentas cerradas antes de AWS: si has AWS cerrado tu cuenta, no podrás volver a abrirla tú mismo. Paga el saldo pendiente en un plazo de 30 días a partir de la fecha en que se cerró tu cuenta y, a continuación, ponte en contacto con nosotros AWS Supportpara volver a abrirla.
- Pagos y cargos: tu cuenta debe tener un método de pago válido y vigente. Como la factura del mes anterior finaliza a principios del mes siguiente, es posible que tengas un saldo pendiente de uso antes del cierre, incluso si tu cuenta no tenía saldo en el momento del cierre. Para revisar o pagar un saldo, consulta Realizar pagos. Cuando vuelvas a abrir tu cuenta, se reanudarán los cargos por todos los servicios que aún estén activos en ella. Si no suspendiste estos servicios antes de cerrar la cuenta, es posible que también hayas incurrido en cargos durante el período posterior al cierre.

¿Cómo volver a abrir tu cuenta

Sigue estos pasos para volver a abrir tu cuenta cerrada.

> **Note**
>
> Esta tarea no es compatible con ninguna operación de API de uno de los AWS SDK. AWS CLI Solo puede realizar esta tarea mediante. Consola de administración de AWS

Para volver a abrir su cuenta desde la página de cuentas

1. Inicia sesión Consola de administración de AWS como usuario root de la cuenta cerrada Cuenta de AWS que deseas volver a abrir. No puedes volver a abrir una cuenta si has iniciado sesión como usuario o rol de IAM.

2. Abre la página de cuentas de la cuenta cerrada de la siguiente manera: En el banner de cuentas cerradas, selecciona Reabrir cuenta.
3. En el cuadro de diálogo Reabrir la cuenta, introduce el ID de cuenta que se muestra en el cuadro de diálogo para confirmar que deseas volver a abrir la cuenta.
4. Seleccione Reabrir cuenta para enviar la solicitud. Un mensaje confirma que se ha iniciado la reapertura de la cuenta.
5. Espera a que se complete la reapertura. Cuando tu cuenta vuelva a estar activa, aparecerá un mensaje confirmando que la cuenta se ha vuelto a abrir correctamente y que se han restablecido tus AWS servicios y tu facturación.

Si no AWS puedes volver a abrir tu cuenta, recibirás una notificación en la consola en la que se te explicará por qué y cómo resolverlo.

¿Qué puedes esperar después de volver a abrir tu cuenta

Tras enviar una solicitud de reapertura, ocurre lo siguiente:

- Para comprobar el estado, actualiza la página de cuentas. Cuando se complete la reapertura, la cuenta aparecerá como activa y el cartel de cuenta cerrada dejará de aparecer.
- Una vez que la cuenta esté activa, AWS restablece el acceso a sus servicios y recursos y se reanuda la facturación.

Prepara tu cuenta para usarla después de volver a abrirla

Algunos recursos y suscripciones no se restauran automáticamente a un estado de ejecución. Una vez que se vuelva a abrir la cuenta, es posible que tengas que hacer lo siguiente para poder reanudar las operaciones normales:

- Inicie cualquier instancia de Amazon EC2 que se haya detenido al cerrar la cuenta. Para obtener más información, consulte Iniciar una instancia en la Guía del usuario de Amazon EC2.
- Restaure las bases de datos de Amazon RDS a partir de las instantáneas creadas al cerrar la cuenta.
- Cancele y vuelva a suscribirse a cualquier suscripción. AWS Marketplace Las suscripciones no se restauran automáticamente al volver a abrir la cuenta.

Disponibilidad por región

Self-service La reapertura de cuentas está disponible en todas las regiones comerciales.

Seguridad en AWS Administración de cuentas

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, se beneficia de una arquitectura de red y centro de datos diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede usar de forma segura. Third-party los auditores prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de . Para obtener más información sobre los programas de cumplimiento que se aplican a la administración de cuentas, consulte Servicios de AWS Alcance por programa de cumplimiento .
- Seguridad en la nube: su responsabilidad está determinada por el AWS servicio que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

El modelo de responsabilidad compartida se aplica a todos Cuentas de AWS. Esto incluye las cuentas Cuentas de AWS que crees usando nuestra nueva AWS experiencia y las cuentas que crees usando nuestra AWS experiencia avanzada.

Esta documentación te ayuda a entender cómo aplicar el modelo de responsabilidad compartida al usar la administración de AWS cuentas. Puede ver cómo configurar Account Management para satisfacer sus objetivos de seguridad y conformidad. También aprenderás a usar otros AWS servicios que te ayudan a supervisar y proteger tus recursos de administración de cuentas. Parte de esta documentación solo es relevante para las cuentas creadas con nuestra AWS experiencia avanzada. Identificaremos cuándo la documentación solo es relevante para las cuentas creadas con nuestra AWS experiencia avanzada.

Temas

- Protección de datos en AWS Administración de cuentas
- AWS PrivateLink for AWS Administración de cuentas
- Identity and Access Management para AWS Administración de cuentas
- AWS políticas administradas para AWS Administración de cuentas

- Validación de conformidad para AWS Administración de cuentas
- Resiliencia en AWS Administración de cuentas
- Seguridad de infraestructura en AWS Account Management

Protección de datos en AWS Administración de cuentas

La siguiente información es relevante para todos Cuentas de AWS.

El modelo de responsabilidad AWS compartida El modelo de responsabilidad se aplica a la protección de datos en la administración de AWS cuentas. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todo el Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de los datos y las condiciones legales de la región de . Para obtener más información sobre la protección de datos en Europa, consulte el Centro del Reglamento General de Protección de Datos (RGPD).

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Úselo SSL/TLS para comunicarse con AWS los recursos. Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Configure el registro de actividad de los usuarios y de la API con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail rutas para capturar AWS actividades, consulte Cómo trabajar con CloudTrail rutas en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados que contiene Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger la información confidencial almacenada en Amazon S3.
- Si necesita módulos criptográficos validados por la FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información

sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabajas con la administración de cuentas o con otros métodos que Servicios de AWS utilizan la consola, la API o los SDK. AWS CLI AWS Cualquier dato que introduzca en etiquetas o campos de formato libre utilizados para los nombres se pueden emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

AWS PrivateLink for AWS Administración de cuentas

La siguiente información es relevante para todos Cuentas de AWS.

Si utiliza Amazon Virtual Private Cloud (Amazon VPC) para alojar sus AWS recursos, puede acceder al servicio de administración de AWS cuentas desde la VPC sin tener que utilizar la red pública de Internet.

Amazon VPC le permite lanzar AWS recursos en una red virtual personalizada. Puede utilizar una VPC para controlar la configuración de red, como el intervalo de direcciones IP, las subredes, las tablas de enrutamiento y las puertas de enlace de red. Para obtener más información sobre VPC, consulte la Guía del usuario de Amazon VPC.

Para conectar Amazon VPC a Account Management, primero debe definir un punto de conexión de VPC de interfaz, lo que le permitirá conectar la VPC a otros servicios de AWS . El punto de conexión ofrece conectividad escalable de confianza sin necesidad de utilizar una gateway de Internet, una instancia de conversión de las direcciones de red (NAT) o una conexión de VPN. Para obtener más información, consulte Puntos de conexión de VPC de la interfaz (AWS PrivateLink) en la Guía del usuario de Amazon VPC.

Creación del punto de conexión

Puede crear un punto de enlace de administración de AWS cuentas en su VPC mediante el AWS SDK Consola de administración de AWS, la API de administración de AWS cuentas, el AWS Command Line Interface (AWS CLI) o. CloudFormation

Para obtener información sobre la creación y configuración de un punto final mediante la consola de Amazon VPC o el AWS CLI, consulte la sección sobre la creación de un punto de enlace de interfaz en la guía del usuario de Amazon VPC.

> **Note**
>
> Cuando crear un punto de conexión, especifique que Account Management es el servicio al que desea que se conecte la VPC, mediante el siguiente formato:
>
> ```
> com.amazonaws.us-east-1.account
> ```
>
> Debe usar la cadena exactamente como se muestra, especificando la región `us-east-1`. Como servicio global, la administración de cuentas solo se aloja en esa AWS región.

Para obtener información sobre cómo crear y configurar un punto de enlace con CloudFormation, consulte el recurso AWS: :EC2: :VPCendpoint en la guía del usuario. CloudFormation

Políticas de punto de conexión de VPC de Amazon

Puede controlar qué acciones se pueden realizar a través de este punto de enlace de servicio adjuntando una política de punto final al crear el punto de enlace de Amazon VPC. Puede crear reglas de IAM complejas al asociar varias políticas de punto de conexión. Para obtener más información, consulte lo siguiente:

- Políticas de punto de conexión de Amazon Virtual Private Cloud para Account Management
- Controlling Access to Services with VPC Endpoints en la Guía de AWS PrivateLink .

Políticas de punto de conexión de Amazon Virtual Private Cloud para Account Management

La siguiente información es relevante para todos Cuentas de AWS.

Puede crear una política de punto de conexión de Amazon VPC para Account Management donde especifique lo siguiente:

- La entidad principal que puede realizar acciones.
- Acciones que las entidades principales pueden realizar.

- El recurso en el que se pueden realizar las acciones.

El siguiente ejemplo muestra una política de puntos de conexión de Amazon VPC que permite a un usuario de IAM llamado Alice de la cuenta 123456789012 recuperar y cambiar la información de contacto alternativa de cualquier cuenta Cuenta de AWS, pero deniega a todos los usuarios de IAM el permiso para eliminar cualquier información de contacto alternativa de cualquier cuenta.

Si desea conceder acceso a las cuentas que forman parte de una AWS organización a un principal que esté en una de las cuentas de los miembros de la organización, el elemento debe utilizar el `Resource` siguiente formato:

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

Para obtener más información sobre cómo crear políticas de puntos de conexión, consulte Controlling Access to Services with VPC Endpoints en la Guía de AWS PrivateLink .

Identity and Access Management para AWS Administración de cuentas

AWS Identity and Access Management (IAM) es una Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. Los administradores de IAM controlan quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de Account Management. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

La siguiente información trata sobre Identity and Access Management para la administración de AWS cuentas. Esta información es especialmente relevante para la Cuentas de AWS que crea cuando utiliza nuestra AWS experiencia avanzada o si ha activado funciones avanzadas en su cuenta. Para obtener más información sobre cómo funciona el control de acceso para nuestra nueva AWS experiencia, consulteCompare la gestión de acceso.

Temas

- Público
- Autenticación con identidades
- Administración del acceso con políticas
- Cómo AWS La administración de cuentas funciona con IAM

- Identity-based ejemplos de políticas para AWS Administración de cuentas
- Uso de políticas basadas en la identidad (políticas de IAM) para AWS Administración de cuentas
- Resolución de problemas AWS Administración de cuentas: identidad y acceso

Público

La forma en que utilizas AWS Identity and Access Management (IAM) varía según tu función:

- Usuario del servicio: solicite permisos al administrador si no puede acceder a las características (consulte Resolución de problemas AWS Administración de cuentas: identidad y acceso).
- Administrador del servicio: determine el acceso de los usuarios y envíe las solicitudes de permiso (consulte Cómo AWS La administración de cuentas funciona con IAM).
- Administrador de IAM: escribe las políticas para administrar el acceso (consulte Identity-based ejemplos de políticas para AWS Administración de cuentas).

Autenticación con identidades

La autenticación es la forma en que inicias sesión AWS con tus credenciales de identidad. Debe autenticarse como usuario de Usuario raíz de la cuenta de AWS IAM o asumir una función de IAM.

Puede iniciar sesión como una identidad federada con las credenciales de una fuente de identidad, como AWS IAM Identity Center (IAM Identity Center), la autenticación de inicio de sesión único o las credenciales. Google/Facebook Para obtener más información sobre el inicio de sesión, consulte Cómo iniciar sesión en la Cuenta de AWS en la Guía del usuario de AWS Sign-In .

Para el acceso programático, AWS proporciona un SDK y una CLI para firmar criptográficamente las solicitudes. Para obtener más información, consulte AWS Signature Version 4 para solicitudes de API en la Guía del usuario de IAM.

Cuenta de AWS usuario raíz

Al crear una Cuenta de AWS, se comienza con una identidad de inicio de sesión denominada usuario Cuenta de AWS raíz, que tiene acceso completo a todos los Servicios de AWS recursos. Se recomiendaencarecidamente que no utilice el usuario raíz para las tareas diarias. Para ver las tareas que requieren credenciales de usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio empresarial, del proveedor de identidades web o al Directory Service que se accede Servicios de AWS mediante credenciales de una fuente de identidad. Las identidades federadas asumen roles que proporcionan credenciales temporales.

Para una administración de acceso centralizada, se recomienda AWS IAM Identity Center. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad con permisos específicos para una sola persona o aplicación. Recomendamos el uso de credenciales temporales en lugar de usuarios de IAM con credenciales de larga duración. Para obtener más información, consulte Exigir a los usuarios humanos que utilicen la federación con un proveedor de identidad para acceder AWS mediante credenciales temporales en la Guía del usuario de IAM.

Un grupo de IAM especifica un conjunto de usuarios de IAM y facilita la administración de los permisos para grupos grandes de usuarios. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un Rol de IAM es una identidad con permisos específicos que proporciona credenciales temporales. Puede asumir un rol cambiando de un rol de usuario a uno de IAM (consola) o llamando a una AWS CLI operación de AWS API. Para obtener más información, consulte Métodos para asumir un rol en la Guía del usuario de IAM.

Los roles de IAM son útiles para el acceso de usuario federado, los permisos de usuario de IAM temporales, el acceso entre cuentas, el acceso entre servicios y las aplicaciones que se ejecutan en Amazon EC2. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Administración del acceso con políticas

AWS Para controlar el acceso, puede crear políticas y adjuntarlas a AWS identidades o recursos. Una política define los permisos cuando están asociados a una identidad o un recurso. AWS evalúa

estas políticas cuando un director hace una solicitud. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre los documentos de políticas de JSON, consulte Información general de políticas de JSON en la Guía del usuario de IAM.

Mediante las políticas, los administradores especifican quién tiene acceso a qué, definiendo qué entidad principal puede realizar acciones sobre qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM crea políticas de IAM y las agrega a roles, que los usuarios pueden asumir posteriormente. Las políticas de IAM definen permisos independientemente del método que se utilice para realizar la operación.

Identity-based políticas

Identity-based las políticas son documentos de política de permisos de JSON que se adjuntan a una identidad (usuario, grupo o rol). Estas políticas controlan qué acciones pueden realizar las identidades, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Identity-based las políticas pueden ser políticas integradas (integradas directamente en una sola identidad) o políticas administradas (políticas independientes asociadas a varias identidades). Para obtener información sobre cómo elegir entre políticas administradas e insertadas, consulte Selección entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Resource-based políticas

Resource-based las políticas son documentos de políticas de JSON que se adjuntan a un recurso. Los ejemplos incluyen las Políticas de confianza de roles de IAM y las Políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Debe especificar una entidad principal en una política basada en recursos.

Resource-based las políticas son políticas en línea que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Otros tipos de políticas

AWS admite tipos de políticas adicionales que pueden establecer los permisos máximos que conceden los tipos de políticas más comunes:

- Límites de permisos: establecen los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM. Para obtener más información, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): especifican los permisos máximos para una organización o unidad organizativa en AWS Organizations. Para obtener más información, consulte Políticas de control de servicios en la Guía del usuario de AWS Organizations .
- Políticas de control de recursos (RCP): definen los permisos máximos disponibles para los recursos de las cuentas. Para obtener más información, consulte Políticas de control de recursos (RCP) en la Guía del usuario de AWS Organizations .
- Políticas de sesión: políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal para un rol o un usuario federado. Para obtener más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo AWS La administración de cuentas funciona con IAM

Esta información es la más relevante para la Cuentas de AWS que crea cuando utiliza nuestra AWS experiencia avanzada. Para obtener información sobre cómo funciona el control de acceso para nuestra nueva AWS experiencia, consulteCompare la gestión de acceso.

Antes de utilizar IAM para administrar el acceso a Account Management, descubra qué características de IAM se pueden utilizar con Account Management.

Funciones de IAM que puede utilizar con AWS Administración de cuentas

Característica de IAM	Compatibilidad con Account Management
Identity-based políticas	Sí
Resource-based políticas	No

Característica de IAM	Compatibilidad con Account Management
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política	Sí
ACL	No
ABAC (etiquetas en políticas)	No
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	No
Service-linked roles	No

Para obtener una visión general de cómo funcionan la administración de cuentas y otros AWS servicios con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Identity-based políticas de gestión de cuentas

Compatibilidad con las políticas basadas en identidad: sí

Identity-based las políticas son documentos de política de permisos de JSON que puedes adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de la política de JSON de IAM en la Guía del usuario de IAM.

Identity-based ejemplos de políticas para la administración de cuentas

Para ver ejemplos de políticas basadas en identidades de Account Management, consulte Identity-based ejemplos de políticas para AWS Administración de cuentas.

Resource-based políticas dentro de la administración de cuentas

Admite políticas basadas en recursos: no

Resource-based las políticas son documentos de políticas de JSON que se adjuntan a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política basada en recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Acciones de política para Account Management

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de administración de cuentas, consulta las acciones definidas por la administración de AWS cuentas en la Referencia de autorización de servicios.

Las acciones de política de Account Management utilizan el siguiente prefijo antes de la acción.

```
account
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

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

Puede utilizar caracteres comodín (*) para especificar varias acciones . Por ejemplo, para especificar todas las acciones que funcionan con los contactos alternativos Cuenta de AWS de una persona, incluye la siguiente acción.

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

Para ver ejemplos de políticas basadas en identidades de Account Management, consulte Identity-based ejemplos de políticas para AWS Administración de cuentas.

Recursos de políticas para Account Management

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). En el caso de las acciones que no admiten permisos por recurso, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

El servicio de administración de cuentas admite los siguientes tipos de recursos específicos como `Resource` elemento de una política de IAM para ayudarle a filtrar la política y distinguir entre estos tipos de Cuentas de AWS recursos:

- account

  Este tipo de `resource` solo coincide con las Cuentas de AWS independientes que no son cuentas de miembro de una organización administrada por el servicio AWS Organizations .
- accountInOrganization

Este `resource` tipo solo coincide con Cuentas de AWS las cuentas de los miembros de una organización gestionada por el AWS Organizations servicio.

Para ver una lista de los tipos de recursos de administración de cuentas y sus ARN, consulte los recursos definidos por la administración de AWS cuentas en la Referencia de autorización del servicio. Para saber con qué acciones puede especificar el ARN de cada recurso, consulte Acciones definidas por la administración de AWS cuentas.

Para ver ejemplos de políticas basadas en identidades de Account Management, consulte Identity-based ejemplos de políticas para AWS Administración de cuentas.

Claves de condición de política para Account Management

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` especifica cuándo se ejecutan las instrucciones en función de criterios definidos. Puede crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

El servicio Account Management admite las siguientes claves de condición de servicios que puede utilizar para ofrecer un filtrado detallado para sus políticas de IAM:

- cuenta: TargetRegion

  Esta clave de condición utiliza un argumento que consiste en una lista de códigos de región de AWS. Permite filtrar la política para que repercuta únicamente en las acciones que se aplican a las regiones especificadas.
- cuenta: AlternateContactTypes

  Esta clave de condición contiene una lista de tipos de contacto alternativos:
  - FACTURACIÓN
  - OPERACIONES
  - SECURITY

El uso de esta clave le permite filtrar la solicitud solo para aquellas acciones dirigidas a los tipos de contacto alternativos especificados.

- cuenta: AccountResourceOrgPaths

  Esta clave de condición utiliza un argumento que consiste en una lista de rutas a través de la jerarquía de la organización para llegar a las unidades organizativas (UO) específicas. Permite filtrar la política para que tenga impacto solo en las cuentas de destino de una UO coincidente.

```
o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/*
```

- cuenta: AccountResourceOrgTags

  Esta clave de condición utiliza un argumento que consiste en una lista de claves y valores de etiqueta. Permite filtrar la política para que repercuta solo en las cuentas que son miembro de una organización y que están etiquetadas con las claves y los valores de etiqueta especificados.

- cuenta: EmailTargetDomain

  Esta clave de condición utiliza un argumento que consiste en una lista de dominios de correo electrónico. Permite filtrar la política para que tenga impacto únicamente en las acciones que coinciden con los dominios de correo electrónico especificados. Esta clave de condición distingue entre mayúsculas y minúsculas. Se debe utilizar `StringEqualsIgnoreCase` en lugar de `StringEquals` en el bloque de condiciones de la política para controlar la acción en función del dominio de la dirección de correo electrónico de destino. Este es un ejemplo de política que permite completar la acción `account:StartPrimaryEmailUpdate` cuando el dominio de correo electrónico contiene `example.com` y `company.org` o cualquier combinación de mayúsculas y minúsculas, por ejemplo `EXAMPLE.COM`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowConditionKey",
            "Effect": "Allow",
            "Action": [
                "account:StartPrimaryEmailUpdate"
            ],
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {
```

```
                    "account:EmailTargetDomain": [
                        "example.com",
                        "company.org"
                    ]
                }
            }
        }
    ]
}
```

Para ver una lista de las claves de condición de la administración de cuentas, consulte las claves de condición de la administración de AWS cuentas en la Referencia de autorización de servicios. Para saber con qué acciones y recursos puede utilizar una clave condicionada, consulte Acciones definidas por la administración de AWS cuentas.

Para ver ejemplos de políticas basadas en identidades de Account Management, consulte Identity-based ejemplos de políticas para AWS Administración de cuentas.

Listas de control de acceso en Account Management

Compatibilidad con ACL: no

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Attribute-based control de acceso con administración de cuentas

Compatibilidad con ABAC (etiquetas en las políticas): no

Attribute-based el control de acceso (ABAC) es una estrategia de autorización que define los permisos en función de los atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para la administración de AWS cuentas, el control de acceso basado en etiquetas solo se admite a través de la clave de `account:AccountResourceOrgTags/key-name` condición. La clave de condición `aws:ResourceTag/key-name` estándar no es compatible con las API del espacio de nombres de la cuenta.

Ejemplo de política de JSON con la clave de condición admitida

El siguiente ejemplo de política permite acceder a la información de contacto de las cuentas etiquetadas con la clave «» CostCenter y el valor «12345" o «67890" en su organización.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "account:GetContactInformation",
            "account:GetAlternateContact"
         ],
         "Resource":"*",
         "Condition":{
            "ForAnyValue:StringEquals":{
               "account:AccountResourceOrgTags/CostCenter":[
                  "12345",
                  "67890"
               ]
            }
         }
      }
   ]
}
```

Para obtener más información sobre ABAC, consulte Definir permisos en función de los atributos con la autorización de ABAC y el tutorial de IAM: Definir permisos de acceso a los AWS recursos en función de las etiquetas en la Guía del usuario de IAM.

Uso de credenciales temporales con Account Management

Compatibilidad con credenciales temporales: sí

Las credenciales temporales proporcionan acceso a AWS los recursos a corto plazo y se crean automáticamente cuando se utiliza la federación o se cambia de rol. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM y Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Cross-service permisos principales para la administración de cuentas

Admite sesiones de acceso directo (FAS): sí

Las sesiones de acceso directo (FAS) utilizan los permisos del operador principal que realiza la llamada Servicio de AWS, junto con los de solicitud, Servicio de AWS para realizar solicitudes a los servicios descendentes. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Sesiones de acceso directo.

Roles de servicio para Account Management

Compatible con roles de servicio: No

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Crear un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

Service-linked funciones de administración de cuentas

Compatibilidad con roles vinculados al servicio: no

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir la función de realizar una acción en su nombre. Service-linked las funciones aparecen en su nombre Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulta Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya una `Yes` en la columna de Service-linked funciones. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Identity-based ejemplos de políticas para AWS Administración de cuentas

Esta información es más relevante para la Cuentas de AWS que crea cuando utiliza nuestra AWS experiencia avanzada. Para obtener información sobre cómo funciona el control de acceso para nuestra nueva AWS experiencia, consulteCompare la gestión de acceso.

De forma predeterminada, los usuarios y roles no tienen permiso para crear ni modificar recursos de Account Management. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por la administración de cuentas, incluido el formato de los ARN de cada uno de los tipos de recursos, consulte las acciones, los recursos y las claves de condición de la administración de AWS cuentas en la Referencia de autorización de servicios.

Temas

- Prácticas recomendadas sobre las políticas
- Mediante la página de cuenta del Consola de administración de AWS
- Proporcionar acceso de solo lectura a la página de la cuenta en Consola de administración de AWS
- Proporcionar acceso completo a la página de la cuenta en Consola de administración de AWS

Prácticas recomendadas sobre las políticas

Identity-based las políticas determinan si alguien puede crear, acceder o eliminar los recursos de administración de cuentas de su cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso.

Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.

- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Mediante la página de cuenta del Consola de administración de AWS

Para acceder a la página de la cuenta en Consola de administración de AWS, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre su Cuenta de AWS. Si crea una política basada en identidad que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles de IAM) que tengan esa política.

Para garantizar que los usuarios y los roles puedan usar la consola de administración de cuentas, puede optar por adjuntar la política `AWSAccountManagementFullAccess` AWS gestionada `AWSAccountManagementReadOnlyAccess` o la política gestionada a las entidades. Para obtener más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

No es necesario permitir permisos mínimos de consola a los usuarios que solo realizan llamadas a la AWS CLI o la AWS API. En su lugar, en muchos casos, puede optar por permitir el acceso únicamente a las acciones que coincidan con las operaciones de la API que está intentando realizar.

Proporcionar acceso de solo lectura a la página de la cuenta en Consola de administración de AWS

En el siguiente ejemplo, desea conceder acceso de solo lectura a un usuario de IAM de su Cuenta de AWS a la página de la cuenta en la Consola de administración de AWS. Los usuarios que tienen esta política adjunta no pueden realizar ningún cambio.

La acción `account:GetAccountInformation` permite acceder a la mayoría de los ajustes de la página de la cuenta. Sin embargo, para ver las regiones de AWS actualmente habilitadas, también debe incluir la acción `account:ListRegions`.

JSON

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

Proporcionar acceso completo a la página de la cuenta en Consola de administración de AWS

En el siguiente ejemplo, desea conceder acceso completo a un usuario de IAM de su Cuenta de AWS a la página de la cuenta en la Consola de administración de AWS. Los usuarios con esta política asociada pueden modificar la configuración de la cuenta.

Esta política de ejemplo se basa en la política del ejemplo anterior y agrega todos los permisos de escritura disponibles (con la excepción de CloseAccount), lo que permite al usuario cambiar la mayoría de los ajustes de la cuenta, incluidos los `account:DisableRegion` permisos `account:EnableRegion` y.

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": "*"
        }
    ]
}
```

Uso de políticas basadas en la identidad (políticas de IAM) para AWS Administración de cuentas

Esta información es más relevante para la Cuentas de AWS que crea cuando utiliza nuestra experiencia avanzada. AWS Para obtener información sobre cómo funciona el control de acceso para nuestra nueva AWS experiencia, consulteCompare la gestión de acceso.

Para obtener información completa sobre los usuarios Cuentas de AWS de IAM, consulte ¿Qué es la IAM? en la Guía del usuario de IAM.

Para obtener instrucciones acerca de cómo actualizar las políticas administradas por el cliente, consulte Edición de políticas de IAM en la Guía del usuario de IAM.

AWS Acciones y políticas de administración de cuentas

En la siguiente tabla, se resumen los permisos que conceden acceso a la configuración de su cuenta. Para ver ejemplos de políticas que utilizan estos permisos, consulte Identity-based ejemplos de políticas para AWS Administración de cuentas.

> **Note**
>
> Para conceder a los usuarios de IAM acceso de escritura a una configuración de cuenta específica en la página Cuenta del usuario Consola de administración de AWS, debe conceder el `GetAccountInformation` permiso, además del permiso (o los permisos) que desee utilizar para modificar esa configuración.

Nombre del permiso	Nivel de acceso	Description (Descripción)
`account:ListRegions`	Enumeración	Concede permiso para enumerar las regiones disponibles.
`account:GetAccount Information`	Lectura	Concede permiso para recuperar la información de una cuenta.

Nombre del permiso	Nivel de acceso	Description (Descripción)
`account:GetAlternateContact`	Lectura	Concede permiso para recuperar los contactos alternativos de una cuenta.
`account:GetContactInformation`	Lectura	Concede permiso para recuperar la información de contacto principal de una cuenta.
`account:GetPrimaryEmail`	Lectura	Concede permiso para recuperar la dirección de correo electrónico principal de una cuenta.
`account:GetRegionOptStatus`	Lectura	Concede permiso para obtener el estado de suscripción de una región.
`account:AcceptPrimaryEmailUpdate`	Escritura	Otorga permiso para aceptar la actualización de la dirección de correo electrónico principal de la cuenta del miembro de una AWS organización.
`account:CloseAccount`	Escritura	Concede permiso para cerrar una cuenta. **Note** Este es un permiso solo para la consola. No hay acceso de API disponible para este permiso.

Nombre del permiso	Nivel de acceso	Description (Descripción)
`account:DeleteAlternateContact`	Escritura	Concede permiso para eliminar los contactos alternativos de una cuenta.
`account:DisableRegion`	Escritura	Concede permiso para deshabilitar el uso de una región.
`account:EnableRegion`	Escritura	Concede permiso para habilitar el uso de una región.
`account:PutAccountName`	Escritura	Concede permiso para actualizar el nombre de una cuenta.
`account:PutAlternateContact`	Escritura	Concede permiso para modificar los contactos alternativos de una cuenta.
`account:PutContactInformation`	Escritura	Concede permiso para actualizar la información de contacto principal de una cuenta.
`account:SendPhoneNumberVerification`	Escritura	Otorga permiso para enviar un código de verificación al número de teléfono de contacto principal de una cuenta.
`account:StartPrimaryEmailUpdate`	Escritura	Otorga permiso para iniciar la actualización de la dirección de correo electrónico principal de la cuenta del miembro de una AWS organización.

Nombre del permiso	Nivel de acceso	Description (Descripción)
`account:VerifyPhoneNumber`	Escritura	Concede permiso para verificar el número de teléfono de contacto principal de una cuenta mediante el envío de un código de verificación.

Resolución de problemas AWS Administración de cuentas: identidad y acceso

Esta información es la más relevante para la Cuentas de AWS que crea cuando utiliza nuestra AWS experiencia avanzada. Para obtener información sobre cómo funciona el control de acceso para nuestra nueva AWS experiencia, consulteCompare la gestión de acceso.

Utilice la siguiente información para diagnosticar y resolver los problemas comunes que pueden surgir cuando trabaja con Account Management e IAM.

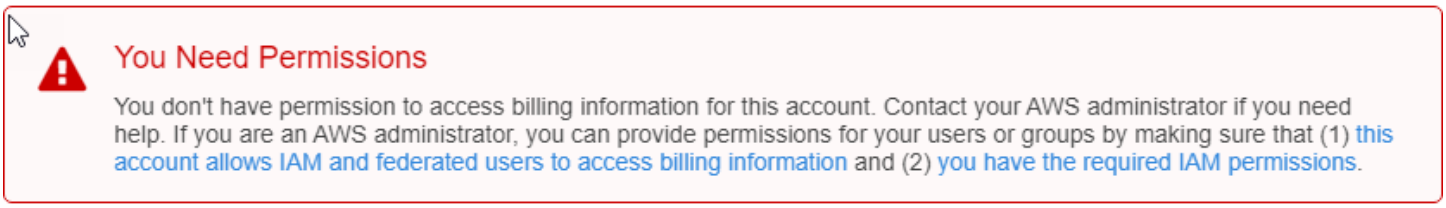
Temas

- No tengo autorización para realizar una acción en la página de la cuenta
- No estoy autorizado a realizar tareas como: PassRole
- Quiero permitir que personas ajenas a mi Cuenta de AWS para acceder a los detalles de mi cuenta

No tengo autorización para realizar una acción en la página de la cuenta

Si Consola de administración de AWS le indica que no está autorizado a realizar una acción, debe ponerse en contacto con su administrador para obtener ayuda. El administrador es la persona que le facilitó el nombre de usuario y la contraseña.

El siguiente ejemplo de error se produce cuando el usuario de `mateojackson` IAM intenta utilizar la consola para ver los detalles sobre su cuenta Cuenta de AWS en la página de cuentas del usuario Consola de administración de AWS , pero no tiene los `account:GetAccountInformation` permisos.



En este caso, Mateo pide a su administrador que actualice sus políticas de forma que pueda obtener acceso al recurso *my-example-widget* mediante la acción `account:GetWidget`.

No estoy autorizado a realizar tareas como: `PassRole`

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, debe actualizar las políticas para poder transferir un rol a Account Management.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir la función al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en Account Management. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

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

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mi Cuenta de AWS para acceder a los detalles de mi cuenta

Se puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Se puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para obtener información acerca de si Account Management admite estas características, consulte Cómo AWS La administración de cuentas funciona con IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a través de los Cuentas de AWS que eres propietario, consulta Cómo proporcionar acceso a un usuario de IAM en otro usuario de tu Cuenta de AWS propiedad en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

AWS políticas administradas para AWS Administración de cuentas

Esta información es especialmente relevante para la Cuentas de AWS que creas cuando utilizas nuestra AWS experiencia avanzada o si has activado las funciones avanzadas de tu cuenta. Para obtener más información sobre cómo funciona el control de acceso en nuestra nueva AWS experiencia, consultaCompare la gestión de acceso.

AWS La administración de cuentas actualmente ofrece dos políticas AWS administradas que están disponibles para su uso:

- AWS política gestionada: AWSAccountManagementReadOnlyAccess
- AWS política gestionada: AWSAccountManagementFullAccess
- Actualizaciones de administración de cuentas para AWS políticas administradas

Una política AWS gestionada es una política independiente creada y administrada por AWS. AWS las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen

todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando haya nuevas operaciones de API disponibles para los servicios existentes.

Para obtener más información, consulte Políticas administradas por AWS en la Guía del usuario de IAM.

AWS política gestionada: AWSAccountManagementReadOnlyAccess

Puede asociar la política `AWSAccountManagementReadOnlyAccess` a las identidades de IAM.

Esta política proporciona permisos de solo lectura únicamente para ver lo siguiente:

- Los metadatos sobre su Cuentas de AWS
- Los Regiones de AWS que están habilitados o deshabilitados para Cuenta de AWS (solo puede ver el estado de las regiones en su cuenta desde la AWS consola)

Para hacerlo, concede permiso para ejecutar cualquiera de las operaciones `Get*` o`List*`. No permite modificar los metadatos de la cuenta ni habilitar o deshabilitar Regiones de AWS la cuenta.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `account`— Permite a los directores recuperar la información de metadatos sobre Cuentas de AWS. También permite a las entidades principales enumerar las Regiones de AWS que están habilitadas para la cuenta en la Consola de administración de AWS.

JSON

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

```
        {
            "Effect": "Allow",
            "Action": [
                "account:Get*",
                "account:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS política gestionada: AWSAccountManagementFullAccess

Puede asociar la política `AWSAccountManagementFullAccess` a las identidades de IAM.

Esta política proporciona acceso administrativo completo para ver o modificar lo siguiente:

- Los metadatos sobre su Cuentas de AWS
- Los Regiones de AWS que están habilitados o deshabilitados para Cuenta de AWS (solo puedes ver el estado o habilitar o deshabilitar las regiones en tu cuenta desde la AWS consola)

Para ello, concede permiso para ejecutar cualquier operación de `account`.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `account`— Permite a los directores ver o modificar la información de los metadatos sobre Cuentas de AWS. También permite a las entidades principales enumerar las Regiones de AWS que están habilitadas para la cuenta y habilitarlas o deshabilitarlas en la Consola de administración de AWS.

JSON

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

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

Actualizaciones de administración de cuentas para AWS políticas administradas

Consulta los detalles sobre las actualizaciones de las políticas AWS administradas para la administración de cuentas desde que este servicio comenzó a rastrear estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de historial de documentos de Account Management.

Cambio	Descripción	Fecha
AWS La administración de cuentas se lanzó con nuevas políticas AWS administradas y comenzó a rastrear los cambios	La administración de cuentas se lanzó inicialmente con las siguientes políticas AWS administradas: • AWSAccountManagementReadOnlyAccess • AWSAccountManagementFullAccess	30 de septiembre de 2021

Validación de conformidad para AWS Administración de cuentas

Nuestra nueva AWS experiencia no se puede utilizar para ninguna carga de trabajo regulada. La siguiente información solo es relevante para las cuentas creadas al usar la opción de registro AWS (avanzada).

Third-party los auditores evalúan la seguridad y el cumplimiento de AWS los servicios que se pueden ejecutar en su Cuenta de AWS empresa como parte de varios programas de AWS cumplimiento. Estos incluyen SOC, PCI, FedRAMP, HIPAA y otros.

Para obtener una lista de AWS los servicios incluidos en el ámbito de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento . Para obtener información general, consulte Programas AWS de cumplimiento Programas .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en la AWS Artifact

Su responsabilidad de cumplimiento al utilizar sus servicios Cuenta de AWS está determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y normativas aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseñar la arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: este documento técnico describe cómo las empresas pueden utilizarlos para crear aplicaciones. AWS HIPAA-eligible

  > **Note**
  >
  > No todos cumplen con los requisitos de la HIPAA. Servicios de AWS Para más información, consulte la Referencia de servicios compatibles con HIPAA.

- AWS Recursos de : esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- Cómo evaluar los recursos con las reglas de la guía para AWS Config desarrolladores: el AWS Config servicio evalúa si las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub CSPM— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interna, lo AWS que le ayuda a comprobar el cumplimiento de los estándares y las mejores prácticas del sector de la seguridad.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia en AWS Administración de cuentas

La siguiente información es relevante para todos Cuentas de AWS. Si utilizas nuestra nueva AWS experiencia, se aplicarán consideraciones regionales adicionales. Para obtener más información, consulte Regiones de AWS para tus proyectos.

La infraestructura AWS global se basa en Regiones de AWS zonas de disponibilidad. Las regiones proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja demora. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre Regiones de AWS las zonas de disponibilidad, consulte Infraestructura AWS global.

Seguridad de infraestructura en AWS Account Management

La siguiente información es relevante para todos Cuentas de AWS.

Como servicios gestionados, AWS los servicios que se ejecutan en usted Cuenta de AWS están protegidos por la seguridad de red AWS global. Para obtener información sobre los servicios de AWS seguridad y cómo AWS protege la infraestructura, consulta AWS Cloud Security. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Las llamadas a la API AWS publicadas se utilizan para acceder a la configuración de la cuenta a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con un secreto directo perfecto (PFS), como el DHE (efímero) o el ECDHE (efímero de curva elíptica Diffie-Hellman). Diffie-Hellman La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puedes utilizar AWS

Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Supervise su Cuenta de AWS

Esto incluye las cuentas Cuentas de AWS que crees con nuestra nueva AWS experiencia y las cuentas que crees con nuestra AWS experiencia avanzada. Para comparar las opciones de registro, consultaCompara las opciones de registro.

La supervisión es una parte importante para mantener la confiabilidad, la disponibilidad y el rendimiento de la administración de AWS cuentas y sus demás AWS soluciones. AWS proporciona las siguientes herramientas de supervisión para supervisar la administración de cuentas, informar cuando algo va mal y tomar medidas automáticas cuando sea necesario:

- AWS CloudTrailcaptura (registra) las llamadas a la API y los eventos relacionados realizados por usted o en su nombre Cuenta de AWS y escribe los archivos de registro en el bucket de Amazon Simple Storage Service (Amazon S3) que especifique. Con esto puede identificar qué usuarios y cuentas llamaron a AWS, la dirección IP de origen de las llamadas y el momento en que se hicieron. Para obtener más información, consulte la Guía del usuario de AWS CloudTrail.
- Amazon EventBridge añade automatización adicional a sus AWS servicios al responder automáticamente a los eventos del sistema, como los problemas de disponibilidad de las aplicaciones o los cambios en los recursos. Los eventos de AWS los servicios se entregan EventBridge prácticamente en tiempo real. Puede crear reglas sencillas para indicar qué eventos le resultan de interés, así como qué acciones automatizadas se van a realizar cuando un evento cumple una de las reglas. Para obtener más información, consulte la Guía del EventBridge usuario de Amazon.

Registro AWS Llamadas a la API de administración de cuentas mediante AWS CloudTrail

Esto incluye las cuentas Cuentas de AWS que crees con nuestra nueva AWS experiencia y las cuentas que crees con nuestra AWS experiencia avanzada. Para comparar las opciones de registro, consultaCompara las opciones de registro.

Las API de administración de AWS cuentas están integradas en un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio que llama a una operación de administración de cuentas. AWS CloudTrail CloudTrailcaptura todas las llamadas a la API de administración de cuentas como eventos. Las llamadas capturadas incluyen todas las llamadas a las operaciones de Account Management. Si crea un registro, puede activar la

entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos para las operaciones de administración de cuentas. Si no configuras un registro, puedes seguir viendo los eventos más recientes en la CloudTrail consola, en el Historial de eventos. Con la información recopilada por CloudTrail, puedes determinar la solicitud que llevó a una operación de administración de cuentas, la dirección IP utilizada para realizar la solicitud, quién la hizo y cuándo, y otros detalles.

Para obtener más información CloudTrail, consulta la Guía AWS CloudTrail del usuario.

Información de administración de cuentas en CloudTrail

CloudTrail se activa en su Cuenta de AWS momento de crear la cuenta. Cuando se produce actividad en una operación de administración de cuentas, CloudTrail registra esa actividad en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puedes ver, buscar y descargar los eventos recientes en tu Cuenta de AWS. Para obtener más información, consulta Visualización de eventos con el historial de CloudTrail eventos.

Para obtener un registro continuo de tus eventos Cuenta de AWS, incluidos los eventos relacionados con las operaciones de administración de cuentas, crea un registro. Un registro permite CloudTrail enviar archivos de registro a un bucket de Amazon S3. De forma predeterminada, al crear una ruta en el Consola de administración de AWS, la ruta se aplica a todos Regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. Puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y tomar medidas en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail servicios e integraciones compatibles
- Configurar las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones
- Recibir archivos de CloudTrail registro de varias cuentas

AWS CloudTrail registra todas las operaciones de la API de administración de cuentas que se encuentran en la sección de referencia de API de esta guía. Por ejemplo, las llamadas a las `CreateAccount` `PutAlternateContact` operaciones y generan entradas en los archivos de CloudTrail registro. `DeleteAlternateContact`

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario raíz o de usuario AWS Identity and Access Management (IAM)
- Si la solicitud se realizó con credenciales de seguridad temporales de una función de IAM o fue un usuario federado
- Si la solicitud la hizo otro servicio AWS

Para obtener más información, consulte el elemento userIdentity de CloudTrail .

Descripción de las entradas de registros de Account Management

Un registro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una única solicitud de cualquier fuente e incluye información sobre la operación solicitada, la fecha y la hora de la operación, los parámetros de la solicitud, etc. CloudTrail los archivos de registro no son un seguimiento ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

Ejemplo 1: El siguiente ejemplo muestra una entrada de CloudTrail registro para una llamada a la `GetAlternateContact` operación destinada a recuperar el contacto `OPERATIONS` alternativo actual de una cuenta. Los valores devueltos por la operación no se incluyen en la información registrada.

Example Ejemplo 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"
}
```

Ejemplo 2: El siguiente ejemplo muestra una entrada de CloudTrail registro para una llamada a la `PutAlternateContact` operación para agregar un nuevo contacto `BILLING` alternativo a una cuenta.

```
{
  "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"
}
```

Ejemplo 3: El siguiente ejemplo muestra una entrada de CloudTrail registro para una llamada a la `DeleteAlternateContact` operación destinada a eliminar el contacto `OPERATIONS` alternativo actual.

```
{
  "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"
}
```


Supervisión de los eventos de administración de cuentas con EventBridge

Esto incluye las cuentas Cuentas de AWS que crees con nuestra nueva AWS experiencia y las cuentas que crees con nuestra AWS experiencia avanzada. Para comparar las opciones de registro, consultaCompara las opciones de registro.

Amazon EventBridge, que antes se llamaba CloudWatch Events, le ayuda a supervisar los eventos que son específicos y a iniciar acciones específicas que utilizan otros Servicios de AWS. Los eventos de Servicios de AWS se envían a casi EventBridge en tiempo real.

Con EventBridge él, puede crear reglas que coincidan con los eventos entrantes y enrutarlos a los destinos para su procesamiento.

Para obtener más información, consulte Cómo empezar a usar Amazon EventBridge en la Guía del EventBridge usuario de Amazon.

Eventos de Account Management

En los siguientes ejemplos, se muestran eventos para Account Management. Los eventos se producen en la medida de lo posible.

Actualmente, solo están disponibles para la administración de cuentas los eventos específicos para habilitar o deshabilitar las regiones y CloudTrail las llamadas a la API.

Event types (Tipos de eventos)

- Evento para la habilitación y deshabilitación de regiones

Evento para la habilitación y deshabilitación de regiones

Cuando habilita o deshabilita una región en una cuenta, ya sea desde la consola o desde la API, se inicia una tarea asincrónica. La solicitud inicial se registrará como un CloudTrail evento en la cuenta de destino. Además, se enviará un EventBridge evento a la cuenta de llamada cuando se haya iniciado el proceso de activación o desactivación y, de nuevo, una vez que se haya completado cualquiera de los procesos.

En el siguiente ejemplo de evento, se muestra cómo se enviará una solicitud `ENABLED` para indicar que el `2020-09-30` la región `ap-east-1` era una cuenta `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"
   }
}
```

Hay cuatro estados posibles que coinciden con los estados devueltos por las API `GetRegionOptStatus` y `ListRegions`:

- `ENABLED`: la región se ha habilitado correctamente para el `accountId` indicado
- `ENABLING`: la región está en proceso de habilitarse para el `accountId` indicado
- `DISABLED`: la región se ha deshabilitado correctamente para el `accountId` indicado
- `DISABLING`: la región está en proceso de deshabilitarse para el `accountId` indicado

El siguiente ejemplo de patrón de eventos crea una regla que captura todos los eventos de la región.

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

El siguiente patrón de eventos de ejemplo crea una regla que captura solo `ENABLED` los eventos de una `DISABLED` región.

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

```
      "status":[
         "DISABLED",
         "ENABLED"
      ]
   }
}
```

Cuotas para AWS Account Management

Cuenta de AWS Tiene cuotas predeterminadas, antes denominadas límites, para cada AWS servicio.

La siguiente información sobre las cuotas es para los proyectos que creas si utilizasRegistrarse en AWS (nuevo). Para ajustar una cuota, crea un ticket de soporte. Para obtener más información, consulte Soporte para proyectos.

Recurso	Cuota	Ajustable
Número de proyectos que tienes en el plan gratuito	29	No
Número de proyectos que puedes tener en el plan de pago	299	No
Número de personas con las que puedes compartir un proyecto	500	No
Número de invitaciones a proyectos que puedes aceptar	100	No

La siguiente información sobre las cuotas es para Cuentas de AWS que la crees si te registras mediante el sistema de registro (avanzado). A menos que se indique lo contrario, cada cuota es Región de AWS específica.

Recurso	Cuota
Número máximo de solicitudes `StartPrimaryEmailUpdate` por cuenta de destino	3 por 30 segundos
Número de contactos alternativos en un Cuenta de AWS	3: uno para `BILLING`, uno para `SECURITY` y uno para `OPERATIONS`

Recurso	Cuota
Número de solicitudes simultáneas de suscripción/exclusión de región por cuenta	6
Número de solicitudes simultáneas de suscripción/exclusión de región por organización	50
Tasa de solicitudes `AcceptPrimaryEmailUpdate` por cuenta que llama	1 por segundo, ampliación a 1 por segundo
Tasa de solicitudes `DeleteAlternateContact` por cuenta	1 por segundo, ampliación a 6 por segundo
Tasa de solicitudes `DisableRegion` por cuenta	1 por segundo, ampliación a 1 por segundo
Tasa de solicitudes `EnableRegion` por cuenta	1 por segundo, ampliación a 1 por segundo
Tasa de solicitudes `GetAccountInformation` por cuenta que llama	3 por segundo, ampliación a 3 por segundo
Tasa de solicitudes `GetAlternateContact` por cuenta	10 por segundo, ampliación a 15 por segundo
Tasa de solicitudes `GetContactInformation` por cuenta	10 por segundo, ampliación a 15 por segundo
Tasa de solicitudes `GetGovCloudAccountInformation` por cuenta	3 por segundo, ampliación a 5 por segundo
Tasa de solicitudes `GetPrimaryEmail` por cuenta que llama	3 por segundo, ampliación a 3 por segundo
Tasa de solicitudes `GetRegionOptStatus` por cuenta	5 por segundo, ampliación a 5 por segundo
Tasa de solicitudes `ListRegions` por cuenta	5 por segundo, ampliación a 5 por segundo

Recurso	Cuota
Tasa de solicitudes `PutAccountName` por cuenta que llama	1 por segundo, ampliación a 1 por segundo
Tasa de solicitudes `PutAlternateContact` por cuenta	5 por segundo, ampliación a 8 por segundo
Tasa de solicitudes `PutContactInformation` por cuenta	5 por segundo, ampliación a 8 por segundo
Tasa de solicitudes `StartPrimaryEmailUpdate` por cuenta que llama	1 por segundo, ampliación a 1 por segundo

Historial de documentos para la Guía del usuario de Account Management

En la siguiente tabla se describen las versiones de la documentación para la administración de AWS cuentas.

Cambio	Descripción	Fecha
Nuevas API de verificación de números de teléfono	Puedes usar las API nuevas SendPhoneNumberVerification y VerifyPhoneNumberlas API para verificar el número de teléfono del contacto principal . La `GetContactInformation` respuesta también incluye un `VerificationStatus` campo nuevo.	1 de octubre de 2026
Valores actualizados de las cuotas de cierre de cuentas	Se corrigió el porcentaje de cuota de cierre de cuentas del 10% al 20% y el mínimo del 10 al 250 en el tema de solución de problemas.	23 de junio de 2026
API de nombres de cuenta nuevos	Soporte para nuevas API de `GetAccountInformation` y `PutAccountName` para ver o modificar un nombre de cuenta.	22 de abril de 2025
Fin del soporte para editar nuevas de verificación de seguridad	Se ha eliminado de la guía el tema Editar tus preguntas sobre problemas de seguridad desde que finalizó el soporte.	6 de enero de 2025
Nuevas API de correo electrónico principales	Compatibilidad con nuevas API de `GetPrimaryEmail` ,	6 de junio de 2024

	StartPrimaryEmailUpdate y AcceptPrimaryEmailUpdate para actualizar de forma centralizada la dirección de correo electrónico del usuario raíz de cualquier cuenta de miembro en AWS Organizations. Para obtener más información, consulte Actualización de la dirección de correo electrónico del usuario raíz para una cuenta de miembro en la Guía del usuario de AWS Organizations .	
Reescritura del tema de cierre de una cuenta	Revisión completa de todo el tema de cierre de cuentas, incluida la adición de pasos sobre cómo cerrar cuentas de miembros y de administración.	1 de febrero de 2024
Fin de la compatibilidad para agregar nuevas preguntas de verificación de seguridad	Nuevo contenido agregado, en el que se indica que la opción de agregar nuevas preguntas de verificación se ha eliminado de la página de la cuenta.	5 de enero de 2024
Fin de la compatibilidad con el espacio de nombres aws-portal	AWS Identity and Access Management (IAM) las acciones que antes se utilizaban para administrar tu cuenta (por ejemplo, aws-portal:ModifyAccount yaws-portal:ViewAccount) han llegado al final del soporte estándar.	1 de enero de 2024

Reescritura del tema de las regiones	Revisión completa de todo el tema de las regiones, incluida la adición de controles de expansión y contracción.	8 de octubre de 2023
Reubicación de los temas para los usuarios raíz en la Guía del usuario de IAM	Consolidación del debate sobre los usuarios raíz en un tema y enlaces de referenci a cruzada agregados a los temas de los usuarios raíz que se trasladaron a la Guía del usuario de IAM.	18 de septiembre de 2023
Nueva sección agregada al tema de contacto de la cuenta principal	Nueva sección de requisito s de número de teléfono y dirección de correo electrónico agregada.	12 de septiembre de 2023
Nuevas API de información de contacto	Compatibilidad con nuevas API `GetContactInformation` y `PutContactInformation` .	22 de julio de 2022
AWS La administración de cuentas ahora permite actualizar contactos alternativos a través de la AWS Organizations consola.	Ahora puedes actualizar los contactos alternativos de tu organización a través de la AWS Organizations consola mediante los permisos de la API de cuentas proporcionados por las políticas AWS Organizations gestionadas actualizadas.	8 de febrero de 2022
Versión inicial	Versión inicial de la guía de referencia sobre la administración de AWS cuentas	30 de septiembre de 2021

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.