



Guía de referencia

AWS Administración de cuentas



AWS Administración de cuentas: Guía de referencia

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 que lo usa? AWS	3
AWS Servicios relacionados	4
Uso del usuario raíz	5
Soporte y comentarios	5
Otros AWS recursos	5
Introducción a su cuenta	7
Revisar los requisitos previos	7
Paso 1: cree su cuenta	8
Paso 2: active la MFA para su usuario raíz	10
Paso 3: cree un usuario administrador	11
Temas relacionados	11
Acceso a su cuenta	11
Planificación de la estructura de gobernanza de su	13
Ventajas de usar múltiples Cuentas de AWS	13
Administrar múltiples Cuentas de AWS	14
Cuándo usar AWS Organizations	15
Habilite el acceso confiable	16
Habilitación de una cuenta de administrador delegado	18
Restrinja el acceso mediante SCPs	19
Cuándo usar AWS Control Tower	21
Descripción de los modos de operación de la API	22
Conceder permisos para actualizar los atributos de la cuenta	23
Configure su cuenta	26
Creación o actualización del alias de cuenta	26
Activar o desactivar Regiones de AWS en tu cuenta	26
Referencia de disponibilidad regional	29
Observaciones antes de habilitar o deshabilitar regiones	32
Tiempos de procesamiento y límites de solicitudes	33
Habilitar o deshabilitar una región para cuentas independientes	33
Habilitar o deshabilitar una región en su organización	36
Actualiza la facturación de tu Cuenta de AWS	38
Actualizar el correo electrónico del usuario raíz	39

Actualizar el correo electrónico del usuario raíz (correo electrónico de) para una cuenta independiente Cuenta de AWS o de administración	40
Actualice el correo electrónico del usuario raíz (correo electrónico de) de cualquier Cuenta de AWS miembro de su organización	41
Actualizar la contraseña del usuario raíz	44
Actualizar tu Cuenta de AWS nombre	45
Actualizar el nombre de tu cuenta para convertirla en una cuenta independiente Cuenta de AWS	46
Actualizar el nombre de tu cuenta para cualquier Cuenta de AWS miembro de tu organización	48
Actualizar los contactos alternativos para su Cuenta de AWS	49
Requisitos de número de teléfono y dirección de correo electrónico	50
Actualice los contactos alternativos para crear uno independiente Cuenta de AWS	51
Actualice los contactos alternativos de cualquiera de los contactos Cuenta de AWS de su organización	54
cuenta: clave de AlternateContactTypes contexto	58
Actualizar el contacto principal de tu Cuenta de AWS	59
Requisitos de número de teléfono y dirección de correo electrónico	59
Actualizar el contacto principal de una cuenta independiente Cuenta de AWS o de administración	60
Actualizar el contacto principal de cualquier cuenta de AWS miembro de tu organización	62
Ve los identificadores de su cuenta	65
Encuentra tu Cuenta de AWS ID	66
Encuentra el seudónimo canónico de tu Cuenta de AWS	68
Protección de su cuenta	72
Protección de datos	73
AWS PrivateLink	74
Creación del punto de conexión	74
Políticas de punto de conexión de VPC de Amazon	75
Políticas de punto de conexión	75
Gestión de identidad y acceso	76
Público	76
Autenticación con identidades	77
Administración del acceso con políticas	78
AWS Administración de cuentas e IAM	80
Ejemplos de políticas basadas en identidades	88

Uso de políticas basadas en identidades	92
Resolución de problemas	95
AWS políticas gestionadas	97
AWSAccountManagementReadOnlyAccess	98
AWSAccountManagementFullAccess	99
Actualizaciones de políticas	99
Validación de conformidad	100
Resiliencia	101
Seguridad de la infraestructura	101
Supervise su cuenta	103
CloudTrail registros	103
Información sobre la administración de cuentas en CloudTrail	104
Descripción de las entradas de registros de Account Management	105
Supervisar los eventos de administración de cuentas con EventBridge	108
Eventos de Account Management	109
Solución de problemas con su cuenta	111
Problemas de creación de cuentas	111
Problemas con el cierre de una cuenta	112
No sé cómo eliminar o cancelar mi cuenta	112
No veo el botón Cerrar cuenta en la página de la cuenta	113
He cerrado mi cuenta, pero aún no he recibido una confirmación por correo electrónico	113
Recibo un mensaje de error ConstraintViolationException «» al intentar cerrar mi cuenta	113
Recibo el mensaje de error "CLOSE_ACCOUNT_QUOTA_EXCEEDED" cuando intento cerrar una cuenta de miembro	114
¿Debo eliminar mi AWS organización antes de cerrar la cuenta de administración?	114
Otros problemas.	114
Necesito cambiar la tarjeta de crédito de mi Cuenta de AWS	114
Necesito denunciar una Cuenta de AWS actividad fraudulenta	115
Necesito cerrar mi Cuenta de AWS	115
Cierre su cuenta	116
Qué debe saber antes de cerrar su cuenta	116
Cómo cerrar su cuenta	118
Qué esperar después de cerrar su cuenta	121
Periodo posterior al cierre	122
Reabrir tu Cuenta de AWS	122
referencia de la API	123

Acciones	125
AcceptPrimaryEmailUpdate	127
DeleteAlternateContact	132
DisableRegion	137
EnableRegion	141
GetAccountInformation	145
GetAlternateContact	151
GetContactInformation	157
GetGovCloudAccountInformation	161
GetPrimaryEmail	168
GetRegionOptStatus	172
ListRegions	176
PutAccountName	181
PutAlternateContact	186
PutContactInformation	192
StartPrimaryEmailUpdate	196
Acciones relacionadas	200
CreateAccount	200
CreateGovCloudAccount	200
DescribeAccount	200
Data Types	201
AlternateContact	202
ContactInformation	204
Region	208
ValidationExceptionField	209
Parámetros comunes	209
Errores comunes	212
Realizar solicitudes de consulta HTTP	213
Puntos de conexión	214
HTTPS obligatorio	214
Firmar las solicitudes de AWS la API de administración de cuentas	215
Cuotas	216
Administre las cuentas en India	218
Crea una Cuenta de AWS con AWS India	218
Administre la información de verificación del cliente	221
Compruebe el estado de verificación del cliente	221

Cree la información de verificación del cliente	221
Edite la información de verificación del cliente	222
Documentos de la India aceptados para la verificación del cliente	223
Administre su cuenta en AWS India	224
Historial de revisión	226
.....	ccxxix

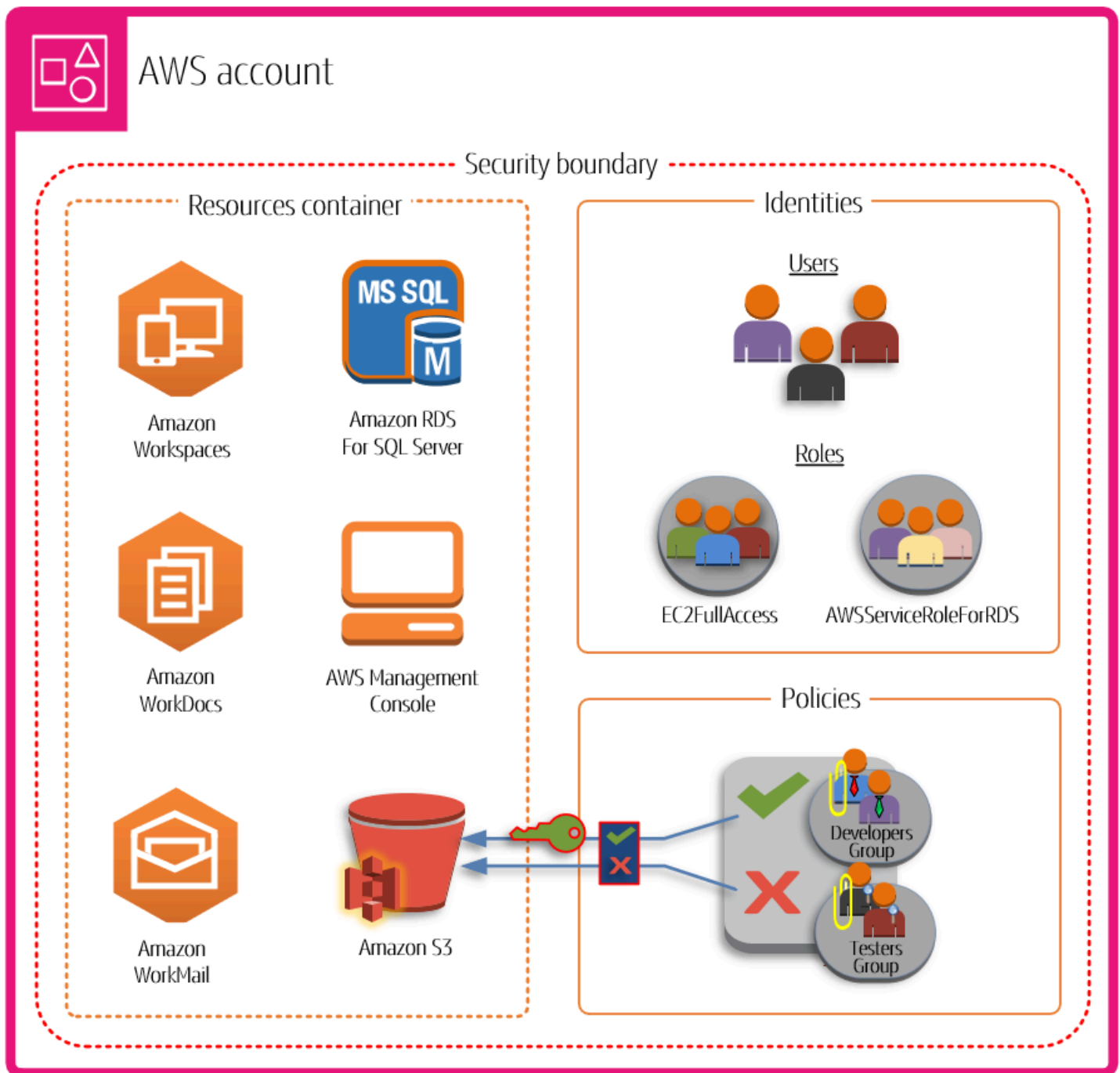
¿Qué es un Cuenta de AWS?

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

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 los AWS servicios. Como se muestra en la siguiente ilustración, y Cuenta de AWS cumple dos funciones principales:

- **Contenedor de recursos:** un Cuenta de AWS es el contenedor básico para todos los AWS recursos que cree como AWS cliente. Por ejemplo, un depósito de Amazon Simple Storage Service (Amazon S3), una base de datos del Amazon Relational Database Service (Amazon RDS) y una instancia de Amazon Elastic Compute Cloud (EC2Amazon) 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:** un 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 varias Cuentas de AWS es una práctica recomendada para escalar su entorno, ya que proporciona un límite natural de facturación de los costos, aísla los recursos para garantizar la seguridad, brinda flexibilidad a las personas y los equipos, además de ser adaptable a los nuevos procesos comerciales. Para obtener más información, consulte [Ventajas de usar múltiples Cuentas de AWS](#).

Características de un Cuenta de AWS

Cuentas de AWS incluyen las siguientes características principales:

- **Supervise y controle los costos:** una cuenta es el medio predeterminado por el que se asignan 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 la elaboración de informes de costes a nivel de cuenta, AWS también cuenta con un soporte integrado para consolidar y elaborar informes sobre los costes de todo el conjunto de cuentas en caso de que decidas 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:** An Cuenta de AWS proporciona límites de seguridad, acceso y facturación para sus AWS recursos que pueden ayudarlo a lograr la autonomía y el aislamiento de los recursos. Por diseño, todos los recursos aprovisionados en una cuenta están aislados de forma lógica de los recursos aprovisionados en otras cuentas, incluso dentro de su 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 que lo usa? AWS

Si es la primera vez que usa AWS, su primer paso es registrarse en un Cuenta de AWS. Cuando te registras, AWS crea una cuenta con los detalles que proporcionas y te asigna la cuenta. Después de crear la suya Cuenta de AWS, inicie sesión como [usuario raíz](#), active la autenticación multifactor (MFA) para el usuario raíz y asigne acceso administrativo a un usuario.

Para step-by-step obtener instrucciones sobre cómo configurar una cuenta nueva, consulte [Cómo empezar con un Cuenta de AWS](#)

AWS Servicios relacionados

Cuentas de AWS trabaje sin problemas con los siguientes servicios:

- IAM

Cuenta de AWS El suyo está estrechamente integrado con AWS Identity and Access Management (IAM). Puede utilizar IAM con su cuenta para asegurarse de que otras personas que trabajan en la cuenta dispongan de todo el acceso que necesitan para hacer su trabajo. También utiliza IAM para controlar el acceso a todos sus 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, le recomendamos configurar varias AWS cuentas que reflejen la estructura específica de la 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 usar AWS Organizations](#).

- AWS Control Tower

AWS Control Tower proporciona una forma simplificada de configurar y gobernar un entorno seguro de múltiples cuentas AWS . AWS Control Tower automatiza la creación de un entorno de múltiples cuentas mediante AWS Organizations la creación de instancias de un conjunto de cuentas iniciales y con algunas configuraciones y barreras predeterminadas para el entorno. Se puede utilizar AWS Control Tower para aprovisionar nuevas cuentas Cuentas de AWS en unos pocos pasos y, al mismo tiempo, garantizar que las cuentas se ajusten a las políticas de la organización. Para obtener más información, consulte [Cuándo usar AWS Control Tower](#).

Uso del Usuario raíz de la cuenta de AWS

Al crear un Cuenta de AWS, se comienza con una identidad de inicio de sesión denominada usuario Cuenta de AWS raíz que tiene acceso completo a todos Servicios de AWS los recursos. Se recomienda encarecidamente 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 root](#) y [crear](#) o [eliminar claves de acceso \(clave de acceso IDs y claves de acceso secretas\)](#) para su usuario root. 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 usuario](#) de AWS inicio de sesión.

Support for AWS Account Management

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 encuentras las respuestas que buscas AWS re:Post, puedes 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](#).

Otros 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, información técnica FAQs, sobre el estado del servicio y AWS Trusted Advisor.
- [AWS Support](#): la página web principal con información sobre AWS Support one-on-one, un canal de soporte 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.

Cómo empezar con un Cuenta de AWS

Si eres nuevo en AWS, el primer paso es registrarte en un Cuenta de AWS. Cuando lo haga, AWS creará una cuenta con los detalles que proporcione y se la asignará.

Los temas de esta sección lo ayudarán a comenzar a conocer y configurar una nueva Cuenta de AWS.

Temas

- [Requisitos previos para crear un nuevo Cuenta de AWS](#)
- [Crea un Cuenta de AWS](#)
- [Activar la MFA para su usuario raíz](#)
- [Creación de un usuario administrador](#)
- [Acceder a su Cuenta de AWS](#)

Requisitos previos para crear un nuevo Cuenta de AWS

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 o producción). Para las cuentas personales, considere la posibilidad de utilizar un estándar de nomenclatura como nombre, apellidos y propósito (por ejemplo, paulo-santos-testaccount).
- 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.

Crea un Cuenta de AWS

Estas instrucciones son para crear un Cuenta de AWS exterior de la India. Para crear una cuenta en la India, consulte [Crea una Cuenta de AWS con 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. Se enviará un código de verificación a la dirección de correo electrónico que ha especificado.

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. Elija Empresarial o Personal. Las cuentas personales y las cuentas empresariales tienen las mismas características y funciones.
6. Introduzca la información de su empresa o su información personal.

 Important

En el caso de las empresas Cuentas de AWS, 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. Lea y acepte el [Acuerdo con el cliente de AWS](#). Asegúrese de leer y comprender los términos del Acuerdo con el AWS cliente.
8. Elija Continuar. En ese momento, recibirás un mensaje de correo electrónico para confirmar Cuenta de AWS que estás listo para usarlo. Puede iniciar sesión en la cuenta nueva con la dirección de correo electrónico y contraseña que proporcionó al registrarse. Sin embargo, no podrás usar ningún AWS servicio hasta que termines de activar tu cuenta.
9. Introduzca la información sobre su método de pago y, a continuación, seleccione Verificar y continuar. 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.
10. Ingrese el código de país o región de la lista y, luego, introduzca un número de teléfono al que se lo pueda llamar en los próximos minutos.
11. Introduzca el código que aparece en el CAPTCHA y, a continuación, presione enviar.
12. Cuando el sistema automatizado se ponga en contacto con usted, introduzca el PIN que reciba y, a continuación, envíelo.

13. Selecciona uno de los AWS Support planes disponibles. Para obtener una descripción de los planes de soporte disponibles y sus beneficios, consulte [Compare Soporte plans](#).
14. Seleccione Completar el registro. Aparece una página de confirmación que indica que su cuenta se está activando.
15. 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.
16. Después de recibir el mensaje de activación, puede iniciar sesión en el para empezar [Consola de administración de AWS](#) a usarlo Servicios de AWS. Para obtener información general sobre cómo administrar la configuración de su cuenta, consulte [Configura tu Cuenta de AWS](#).

AWS CLI & SDKs

Puede crear cuentas de miembros en una organización que se administre AWS Organizations ejecutando la [CreateAccount](#) operación 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.

Activar la MFA para su usuario raíz

Es muy recomendable que active la MFA en el usuario raíz. La MFA reduce drásticamente el riesgo de que alguien acceda a su cuenta sin su autorización.

1. Inicia sesión [Consola de administración de AWS](#) como propietario de la cuenta seleccionando Usuario root e introduciendo tu dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

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 usuario](#) de AWS inicio de sesión.

2. Active MFA para el usuario raíz.

Para obtener instrucciones, consulte [Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz \(consola\)](#) en la Guía del usuario de IAM.

Creación de un usuario administrador

Como no puede restringir lo que puede hacer un usuario raíz, recomendamos que no lo utilice para tareas que no lo requieran de forma explícita. En su lugar, asigne acceso administrativo a un usuario administrativo en IAM Identity Center e inicie sesión con ese usuario administrativo para realizar las tareas administrativas diarias.

Para obtener instrucciones, consulte [Configurar el Cuento de AWS acceso para un usuario administrativo del IAM Identity Center en la Guía del usuario](#) del IAM Identity Center.

Temas relacionados

- Para obtener información sobre cómo proteger las credenciales del usuario raíz, consulte [Proteja las credenciales de usuario raíz](#) en la Guía del usuario de IAM.
- Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte [Tareas que requieren credenciales de usuario raíz](#) en la Guía del usuario de IAM.

Acceder a su Cuenta de AWS

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

Consola de administración de AWS

Consola de administración de AWS Se trata [de](#) una interfaz basada en un navegador que puede utilizar para gestionar 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 de su 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 desea crear scripts que realicen 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 SDKs

AWS SDKs Constan de bibliotecas y código de muestra para varios lenguajes de programación y plataformas (por ejemplo, Java, Python, Ruby, .NET, iOS y Android). Se SDKs encargan de tareas como firmar criptográficamente las solicitudes, gestionar los errores y volver a intentar las solicitudes automáticamente. Para obtener más información acerca de AWS SDKs, incluida la forma de descargarlos e instalarlos, consulte [Herramientas para Amazon Web Services](#).

AWS API de consulta HTTPS de administración de cuentas

La API de consulta HTTPS de administración de AWS cuentas le brinda acceso programático a su 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](#).

Planifique su estructura de Cuenta de AWS gobierno

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 de 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 usar AWS Organizations](#)
- [Cuándo usar AWS Control Tower](#)
- [Descripción de los modos de operación de la API](#)

Ventajas de usar múltiples Cuentas de AWS

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 sus recursos en distintos Cuentas de AWS elementos le 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 una Cuenta de AWS que aloje todos los elementos de su carga de trabajo que estén sujetos a las [normas de seguridad del sector de las tarjetas de pago \(PCI\)](#).
- **Aislamiento:** una Cuenta de AWS es una unidad de protección de seguridad. Los posibles riesgos y amenazas a la seguridad deben estar contenidos dentro y 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. Puedes evitar que los equipos interfieran entre sí moviéndolos para separarlos 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, puede 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. Puede seguir consolidando todas sus facturas en un único pagador (utilizando la facturación unificada) AWS Organizations y, al mismo tiempo, separar las partidas por Cuenta de AWS.
- **Asignación de cuotas:** las cuotas AWS de servicio se imponen por separado para cada uno 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 [Marco de Well-Architected de AWS](#). 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.

Administrar 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](#) un AWS servicio gratuito para gestionar todo lo que hay Cuentas de AWS en su organización.

AWS también ofrece AWS Control Tower, que añade capas de automatización AWS gestionada a Organizations y las 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 usar AWS Organizations](#)
- [Cuándo usar AWS Control Tower](#)

Cuándo usar AWS Organizations

AWS Organizations es un AWS servicio que puedes usar para administrarte Cuentas de AWS como 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 gestionas AWS Organizations tus cuentas como 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. Puede extender esta funcionalidad adicional a otros AWS servicios habilitando el acceso confiable entre Organizations 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 la administración de AWS cuentas](#).

Administrador delegado

Después de habilitar el acceso confiable, también puedes elegir 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 la administración de AWS cuentas](#).

Políticas de control de servicios

Si forma Cuenta de AWS parte de una organización gestionada por AWS Organizations, el administrador de la organización puede aplicar [políticas de control de servicios \(SCPs\)](#) que pueden limitar lo que pueden hacer los directores 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 un rol (principal) en la cuenta de un miembro solo puede realizar las operaciones que se encuentren en la intersección de lo permitido por las SCPs políticas de permisos de la cuenta y las políticas de permisos de IAM asociadas al principal. Por ejemplo, se puede utilizar SCPs para impedir que el principal de una cuenta modifique los contactos alternativos de su propia cuenta.

Por ejemplo, SCPs los que se aplican a Cuentas de AWS, consulte [Restrinja el acceso mediante políticas de control de AWS Organizations servicios](#).

Habilite el acceso confiable para la administración de AWS cuentas

Al habilitar el acceso de confianza 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 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 [Uso AWS Organizations 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 la administración de AWS 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 la administración de AWS 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 de confianza para la administración de AWS cuentas, escriba habilitar para confirmarlo y, a continuación, elija Habilitar el acceso de confianza.

AWS CLI & SDKs

Para habilitar el acceso confiable para la administración de AWS 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](#)

El siguiente ejemplo permite un acceso confiable para la administración de AWS cuentas en la organización de la cuenta que realiza la llamada.

```
$ 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 la administración de AWS cuentas

Habilitas una cuenta de administrador delegado para poder acceder a las operaciones de la AWS API de administración de cuentas de otros miembros. AWS Organizations Después de registrar una cuenta de administrador delegado para su organización, los usuarios y los roles de esa cuenta pueden llamar a las operaciones AWS CLI y del AWS SDK en el espacio de account nombres que pueden funcionar en el modo Organizations al admitir un parámetro opcional. AccountId

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, puedes usar las credenciales de la cuenta 123456789012 para llamar a las operaciones de administración de cuentas AWS CLI y de la API 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

La consola de administración de AWS cuentas no admite esta tarea. Solo puede realizar esta tarea mediante la operación AWS CLI o una operación de API desde una de las AWS SDKs.

Restrinja el acceso mediante políticas de control de AWS Organizations servicios

En este tema se presentan ejemplos que muestran cómo puede utilizar las políticas de control de servicios (SCPs) AWS Organizations para restringir lo que pueden hacer los usuarios y las funciones de las cuentas de 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 :

- [Crear SCPs](#)
- [Adjuntar SCPs a cuentas OUs y](#)
- [Estrategias para 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

El siguiente ejemplo de SCP incluye una condición que compara la ruta organizativa de la cuenta con una lista de dos OUs. Esto impide que el principal de cualquier cuenta OUs de la especificada modifique sus propios contactos alternativos.

Cuándo usar AWS Control Tower

AWS Organizations es el servicio fundamental que le permite administrar y proteger todo su AWS entorno de forma centralizada. Un componente crucial de este enfoque AWS Organizations centrado en lo siguiente es. AWS Control Tower AWS Control Tower actúa como una consola de administración dentro de Organizations, proporcionando una forma simplificada de configurar y gobernar un AWS entorno seguro 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 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 compatible. AWS Este enfoque centralizado de la gestión 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

Las operaciones de la API que funcionan con los atributos Cuenta de AWS de una persona siempre funcionan en uno de estos dos modos de operación:

- **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 cuando llamas 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 contextual de la organización se utiliza automáticamente al incluir 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 AWS CLI y las AWS del SDK pueden funcionar tanto en un 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 añadir, actualizar o eliminar atributos de la cuenta Cuentas de AWS mediante las 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 \(ARN\)](#) de una cuenta Cuenta de AWS que puede incluir en el resource elemento de una declaración de política se construye de forma diferente en función de si la cuenta a la que desea hacer referencia es una cuenta independiente o una cuenta que pertenece 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 Account ID.

- 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.

account: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 encuentren en una de las dos especificadas. OUs

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 de una organización. OUs

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

account: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 clasificar 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, tenga en cuenta que el prefijo de la clave de condición es `account`, aunque esté haciendo referencia a las etiquetas en 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 versión independiente Cuenta de AWS.

Configura tu Cuenta de AWS

En esta sección se incluyen temas que describen cómo administrar su Cuenta de AWS.

Note

Si Cuenta de AWS se creó en la India mediante Amazon Web Services India Private Limited (AWS India), hay otras consideraciones. Para obtener más información, consulte [Administre las cuentas en India](#).

Temas

- [Crear un Cuenta de AWS alias](#)
- [Activar o desactivar Regiones de AWS en tu cuenta](#)
- [Actualiza la facturación de tu Cuenta de AWS](#)
- [Actualizar la dirección de correo electrónico del usuario raíz](#)
- [Actualizar la contraseña del usuario raíz](#)
- [Actualizar tu Cuenta de AWS nombre](#)
- [Actualice los contactos alternativos para su Cuenta de AWS](#)
- [Actualizar el contacto principal de tu Cuenta de AWS](#)
- [Ver Cuenta de AWS identificadores](#)

Crear un Cuenta de AWS alias

Si desea que la URL de sus usuarios de IAM contenga el nombre de su empresa (u otro easy-to-remember identificador) en lugar del Cuenta de AWS ID, puede crear un alias de cuenta.

Para obtener información sobre cómo crear o actualizar un alias de cuenta, consulta Cómo [usar un alias para tu Cuenta de AWS ID](#) en la Guía del usuario de IAM.

Activar o desactivar Regiones de AWS en tu cuenta

Una Región de AWS es una ubicación física en el mundo donde AWS hay varias zonas de disponibilidad. 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 de ellas Región de AWS está aislada físicamente 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 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 de sus cargas de trabajo, consulte AWS Aspectos básicos de varias regiones.](#)

Regiones de AWS en términos generales, se dividen en dos categorías de disponibilidad de 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.
- **Regiones de suscripción:** las regiones que se lanzaron después del 20 de marzo de 2019 se encuentran deshabilitadas de forma predeterminada y se denominan regiones de suscripción. 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 utilizar estas regiones de suscripción voluntaria, primero debe habilitarlas en su 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 la región de suscripción en sus cuentas independientes, consulte [Habilitar o deshabilitar una región para cuentas independientes](#), y para habilitar la región de suscripción en sus cuentas de miembros, consulte [Habilitar o deshabilitar una región en su organización](#).

Cuando te registras en una Cuenta de AWS, te AWS recomienda una región de suscripción voluntaria en función del país de tu dirección de contacto. Los clientes de un país con una región de AWS suscripción voluntaria consultan 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 regiones de AWS suscripción en tu cuenta o elegir deshabilitar la región de suscripción que habilitaste al registrarte.

Al crear una Cuenta de AWS, sus datos y credenciales de IAM se configuran automáticamente para que funcionen en todas las regiones predeterminadas, lo que permite que el usuario raíz y las

identidades de IAM con los permisos adecuados accedan a los AWS servicios de estas regiones con sus credenciales existentes. AWS Las regiones opcionales están deshabilitadas de forma predeterminada y, en un principio, los datos y las credenciales de IAM no están disponibles en esas 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, el usuario raíz y las identidades de IAM pueden 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

Al deshabilitar una región, se deshabilita el acceso de IAM a los recursos de la región. Esto no elimina los recursos en cuestión, que siguen incurriendo en 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 estricto entre las regiones de las distintas 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. Dependiendo 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 la `aws` partición le proporciona acceso a varias regiones de la partición comercial para que pueda lanzar AWS los recursos en las ubicaciones que se ajusten a sus necesidades. 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 una `aws-us-gov` partición le proporciona acceso a la región AWS GovCloud (EE. UU. Oeste) y a la región AWS GovCloud (EE. UU. Este). 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

En las siguientes tablas se enumeran los tipos Regiones de AWS 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

Name	Código	Status
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
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

Name	Código
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
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 puntos de conexión), consulte la [Lista de servicios AWS regionales](#).

Important

AWS recomienda utilizar los puntos finales regionales AWS Security Token Service (AWS STS) en lugar del punto final 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 realizar ningún cambio. Sin embargo, los identificadores de sesión del AWS STS punto final global (<https://sts.amazonaws.com>) solo son válidos si usted Regiones de AWS los habilita o si están habilitados de forma predeterminada. Si quiere habilitar una nueva región para su cuenta, puede utilizar los tokens de sesión de los AWS STS puntos de conexión regionales o activar el AWS STS punto de conexión global para emitir símbolos de sesión que sean válidos en todos los Regiones de AWS países. 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 utilizar todas las regiones de destino en una geografía de inferencia entre regiones, independientemente del estado de opción de región: algunos servicios de AWS IA generativa, como Amazon Bedrock (consulte [Aumente el rendimiento con la inferencia entre regiones](#)) y [Amazon Q Developer \(consulte Procesamiento entre regiones en Amazon Q Developer\)](#), utilizan la [inferencia](#) entre regiones. 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 una 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. Solamente se cobran los recursos que se crean en la nueva región.
- EventBridge Integración con Amazon: puedes suscribirte a las notificaciones de actualización de estado por región en. EventBridge Se creará una EventBridge notificación para cada cambio de estado, lo que permitirá a los clientes automatizar los flujos de trabajo.
- Estado expresivo de suscripción por región: debido a la naturaleza asincrónica de enabling/ disabling una región de suscripción voluntaria, hay cuatro posibles estados para una solicitud de suscripción 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 opción regional completada (habilitada o deshabilitada) depende del aprovisionamiento de los principales servicios subyacentes. AWS Es posible que algunos AWS servicios no se puedan utilizar inmediatamente a pesar del estado en que se encuentren. `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 deshabilitación de una región puede tardar entre unos minutos y 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 suscripción regional abiertas en un momento dado 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, lleve a cabo los pasos del siguiente procedimiento. El siguiente Consola de administración de AWS procedimiento siempre funciona solo en el contexto independiente. Puede usarlo Consola de administración de AWS para ver o actualizar solo las regiones disponibles en la cuenta que utilizó para llamar a la operación.

Consola de administración de AWS

Para habilitar o deshabilitar una región para una región 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`(necesario para ver la lista de Regiones de AWS las que están activadas o desactivadas actualmente).
- `account:EnableRegion`
- `account:DisableRegion`

1. Inicie sesión [Consola de administración de AWS](#) como usuario Usuario raíz de la cuenta de AWS o rol 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 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

Puede activar, desactivar, leer y enumerar el estado de opción regional mediante los siguientes AWS CLI comandos o sus operaciones equivalentes al 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 miembros AWS Organizations, lleve a cabo los pasos del siguiente procedimiento.

Note

Las políticas AWS Organizations gestionadas `AWSOrganizationsReadOnlyAccess` o `AWSOrganizationsFullAccess` se actualizan para permitir el acceso a la administración de AWS cuentas, de APIs forma que usted pueda acceder a los datos de la cuenta desde la AWS Organizations consola. Para ver las políticas administradas actualizadas, consulte [Actualizaciones de las políticas AWS administradas por Organizations](#).

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 al servicio de administración de AWS cuentas. Para configurarlo, consulte [Habilite el acceso confiable para la administración de AWS 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

Puede activar, desactivar, leer y mostrar el estado de suscripción regional de las cuentas de los miembros de la organización mediante los siguientes AWS CLI comandos o sus operaciones equivalentes al 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

Puede actualizar todas sus preferencias de Cuenta de AWS facturación mediante la consola de gestión de costes AWS Billing y la consola de gestión de costes. 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](#):

Actualizar la dirección de correo electrónico del usuario raíz

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 Cuenta de AWS 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:

- **Independiente Cuentas de AWS:** si Cuentas de AWS no está asociado a una organización, puede actualizar el correo electrónico del usuario raíz de mediante la consola AWS de administración. Para obtener información sobre cómo hacerlo, consulte [Actualizar el correo electrónico del usuario raíz 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 el correo electrónico del usuario raíz, el de la cuenta del miembro desde la AWS Organizations consola o mediante programación mediante la CLI AWS & SDKs 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

- [Actualizar el correo electrónico del usuario raíz \(correo electrónico de \) para una cuenta independiente Cuenta de AWS o de administración](#)
- [Actualice el correo electrónico del usuario raíz \(correo electrónico de \) de cualquier Cuenta de AWS miembro de su organización](#)

Actualizar el correo electrónico del usuario raíz (correo electrónico de) para una cuenta independiente Cuenta de AWS o de administración

Para editar la dirección de correo electrónico del usuario raíz, la dirección de para una versión independiente Cuenta de AWS, 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 AWS](#) como 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 AWS CLI ni con una operación de API de uno de los AWS SDKs. Solo puede realizar esta tarea mediante Consola de administración de AWS.

Actualice el correo electrónico del usuario raíz (correo electrónico de) de cualquier Cuenta de AWS miembro de 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 step-by-step obtener instrucciones, siga los pasos que se indican en [Actualizar el correo electrónico del usuario raíz \(correo electrónico de \) para una cuenta independiente Cuenta de AWS o de administración](#).

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 usar 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, la dirección de de una cuenta de miembro mediante la 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 puede acceder a una cuenta de una organización diferente a la que utiliza para llamar a la operación.

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 (), debe utilizar el correo electrónico principal en APIs conjunto en el orden en que se muestran en los ejemplos siguientes.

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

Para editar Cuenta de AWS la contraseña del usuario root, lleve a cabo los pasos del siguiente procedimiento.

Consola de administración de AWS

Para editar la contraseña de su usuario raíz

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 AWS](#) como 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 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 AWS CLI ni con una operación de API de uno de los AWS SDKs. Solo puede realizar esta tarea mediante Consola de administración de AWS.

Actualiza tu Cuenta de AWS nombre

Cuando gestione varias aplicaciones Cuentas de AWS, utilice convenciones de nomenclatura claras y alineadas con las unidades de negocio y las aplicaciones para su identificación y 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, 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. 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).

- Independiente Cuentas de AWS : si Cuentas de AWS no está asociada a una organización, puede actualizar el nombre de su cuenta con Consola de administración de AWS, o con. AWS CLI SDKs

Para obtener información sobre como hacer esto, consulte [Actualizar el nombre de tu cuenta para convertirla en una cuenta 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 Organizations, un usuario de la cuenta de administración o de la cuenta de administrador delegado puede actualizar de forma centralizada el nombre de la cuenta de cualquier miembro de la organización desde la AWS Organizations consola o mediante programación mediante el comando y. AWS CLI SDKs Para obtener información sobre como hacer esto, consulte [Actualizar el nombre de tu cuenta para cualquier Cuenta de AWS miembro de tu organización](#).

Note

Los cambios realizados en una Cuenta de AWS pueden tardar hasta cuatro horas en propagarse a todas partes.

Temas

- [Actualizar el nombre de tu cuenta para convertirla en una cuenta independiente Cuenta de AWS](#)
- [Actualizar el nombre de tu cuenta para cualquier Cuenta de AWS miembro de tu organización](#)

Actualiza el nombre de tu cuenta para convertirla en una cuenta independiente Cuenta de AWS

Para cambiar el nombre de la cuenta de una cuenta independiente Cuenta de AWS, lleve a cabo los pasos del siguiente procedimiento.

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 cuenta para una cuenta independiente

1. Utilice su dirección Cuenta de AWS de correo electrónico y contraseña para iniciar sesión en el [Consola de administración de AWS](#) como si fuera suya 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 cuenta para una cuenta independiente

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 SDKs: [PutAccountName](#)

Actualiza el nombre de tu cuenta para cualquier Cuenta de AWS miembro de tu organización

En el modo AWS Organizations con todas las funciones, los usuarios autorizados de IAM o los roles de IAM tanto en las cuentas de administración como de administración delegada pueden administrar 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, debes 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 al servicio de administración de AWS cuentas. Para configurarlo, consulte [Habilite el acceso confiable para la administración de AWS 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 Organizations en <https://console.aws.amazon.com/organizations/>.
2. En el panel de navegación izquierdo, elija 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](#)

Actualice los contactos alternativos para su Cuenta de AWS

Los contactos alternativos AWS permiten 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 AWS de administración o mediante AWS CLI & SDKs. 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 AWS & SDKs Para obtener información sobre cómo hacerlo, consulta Cómo [actualizar los contactos alternativos de cualquier Cuenta de AWS parte de tu](#) organización.

Temas

- [Requisitos de número de teléfono y dirección de correo electrónico](#)
- [Actualice los contactos alternativos para crear uno independiente Cuenta de AWS](#)
- [Actualice los contactos alternativos de cualquiera de los contactos Cuenta de AWS de su 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: "+= .# | !&-_".

Actualice los contactos alternativos para crear una independiente Cuenta de AWS

Para añadir o editar los contactos alternativos de una versión independiente Cuenta de AWS, lleve a cabo los pasos del siguiente procedimiento. El Consola de administración de AWS procedimiento siguiente siempre funciona solo en el contexto independiente. Puede utilizar el 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 ve la opción Editar, es probable que no haya iniciado sesión como el usuario raíz de la cuenta o como una persona que tiene 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 al 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 con 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`.

Actualice los contactos alternativos de cualquiera de los contactos Cuenta de AWS de su organización

Para agregar o editar los detalles de contacto alternativos de cualquier Cuenta de AWS miembro de su organización, lleve a cabo los pasos del siguiente procedimiento.

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 al servicio de administración de AWS cuentas. Para configurarlo, consulte [Habilite el acceso confiable para la administración de AWS cuentas](#).

Note

Las políticas AWS Organizations gestionadas `AWSOrganizationsReadOnlyAccess` o `AWSOrganizationsFullAccess` se actualizan para permitir el acceso a la gestión de AWS cuentas, de APIs forma que puedas acceder a los datos de la cuenta desde la AWS Organizations consola. Para ver las políticas administradas actualizadas, consulte [Actualizaciones de las políticas AWS administradas por Organizations](#).

Consola de administración de AWS

Para agregar o editar los contactos alternativos de cualquier parte Cuenta de AWS de 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 de 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 al 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 puede acceder a una cuenta en una organización diferente a la que utiliza 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": "CF0"
  }
}
```

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 con 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 utilizar la clave de contexto `account:AlternateContactTypes` para especificar cuál de los tres tipos de facturación permite (o deniega) 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

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.

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 & SDKs. Para obtener información sobre cómo hacerlo, consulte [Actualizar el contacto Cuenta de AWS principal 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 AWS & SDKs 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 de una cuenta independiente Cuenta de AWS o de administración](#)
- [Actualiza el contacto principal de cualquier cuenta de AWS miembro de tu organización](#)

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 (EE. UU./Canadá) o +44 (Reino Unido).

- Los números de teléfono no deben incluir espacios en blanco entre el código de área, el código de intercambio 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 de una cuenta independiente Cuenta de AWS o de administración

Para editar sus datos de contacto principales para una cuenta independiente Cuenta de AWS, 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 el 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 tu contacto principal y convertirlo en uno independiente Cuenta de AWS

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 cuenta de AWS miembro de tu organización

Para editar sus datos de contacto principales en cualquier cuenta de AWS miembro de su organización, lleve a cabo los pasos que se indican a continuación.

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 la administración de AWS cuentas](#).

Consola de administración de AWS

Para editar el contacto principal de cualquier miembro Cuenta de AWS de 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 localice el contacto principal,
4. Seleccione Editar.
5. Cambie los valores de cualquiera de los campos disponibles.
6. 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](#).

- No puede acceder a una cuenta en una organización diferente a la que utiliza 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.

Ver Cuenta de AWS identificadores

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 ID de cuenta en sus [nombres de recursos de Amazon \(ARNs\)](#). La parte de ID de cuenta diferencia los recursos en una cuenta de los recursos en otra. Si es usuario AWS Identity and Access Management (de IAM), puede iniciar sesión en él Consola de administración de AWS con el ID de cuenta o el alias de la cuenta. Si bien la cuenta IDs, al igual que cualquier información de identificación, debe usarse y compartirse con cuidado, no se considera información secreta, sensible o confidencial.

[ID de usuario canónico](#)

Un identificador alfanumérico, por ejemplo 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be, una forma ofuscada del identificador. Cuenta de AWS Puede utilizar 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.

Debe estar autenticado AWS para ver estos identificadores.

Warning

No proporcione sus AWS credenciales (incluidas las contraseñas y las claves de acceso) a un tercero que necesite sus Cuenta de AWS identificadores para compartir AWS recursos con usted. Si lo hace, tendrán el mismo acceso al Cuenta de AWS que tiene usted.

Encuentra tu Cuenta de AWS ID

Puedes encontrar el Cuenta de AWS ID utilizando las teclas () Consola de administración de AWS o las teclas AWS Command Line Interface (AWS CLI). En la consola, la ubicación del ID de cuenta depende de si ha iniciado sesión como usuario raíz o usuario de IAM. El ID de cuenta es el mismo, tanto si ha iniciado sesión como usuario raíz o 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 root

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 mediante 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.

Utilice el [get-caller-identity](#) comando 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 tu 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.

i 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 tu Cuenta de AWS ID mediante el AWS CLI

i 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`

Utilice el [get-caller-identity](#) comando de la siguiente manera.

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

Encuentra el seudónimo canónico de tu Cuenta de AWS

Puede encontrar su seudónimo canónico Cuenta de AWS utilizando el o el. Consola de administración de AWS AWS CLI El seudónimo canónico de una Cuenta de AWS es específico de esa cuenta. Puede recuperar su seudónimo 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. Inicie sesión Consola de administración de AWS como usuario raíz o 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 seudónimo canónico para configurar las listas de control de acceso de Amazon S3 (ACLs).

AWS CLI & SDKs

Para encontrar el seudónimo canónico mediante el AWS CLI

El mismo comando AWS CLI and API funciona para los Usuario raíz de la cuenta de AWS usuarios de IAM o las funciones 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 encontrar el seudónimo canónico mediante el AWS CLI

El mismo comando AWS CLI and API funciona para los Usuario raíz de la cuenta de AWS usuarios de IAM o las funciones 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
```

--output text

```
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

Seguridad en la administración de AWS cuentas

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red 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 utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los [AWS programas](#) de de . Para obtener más información sobre los programas de cumplimiento que se aplican a la administración de cuentas, consulte [Servicios de AWS el alcance por programa de cumplimiento Servicios de AWS](#) .
- Seguridad en la nube: su responsabilidad viene 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 los reglamentos aplicables

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida al utilizar la administración de AWS cuentas. Puede ver cómo configurar Account Management para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus recursos de administración de cuentas.

Temas

- [Protección de datos en la gestión de AWS cuentas](#)
- [AWS PrivateLink para la administración de AWS cuentas](#)
- [Identity and Access Management para la administración de AWS cuentas](#)
- [AWS políticas gestionadas para la gestión de AWS cuentas](#)
- [Validación de conformidad para la gestión de AWS cuentas](#)
- [Resiliencia en la gestión de AWS cuentas](#)
- [Seguridad de la infraestructura en AWS Account Management](#)

Protección de datos en la gestión de AWS cuentas

El [modelo de](#) se aplica a protección de datos en la gestión de AWS cuentas. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los 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 datos](#). Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el [Modelo de responsabilidad compartida de AWS y GDPR](#) en el Blog de seguridad de AWS .

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.
- Se utiliza SSL/TLS para comunicarse con AWS los recursos. Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte [Cómo trabajar con CloudTrail senderos](#) en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados que contienen 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 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 trabaja con la administración de cuentas u otro tipo de Servicios de AWS uso de la consola, la API o. AWS CLI AWS SDKs 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 para la administración de AWS cuentas

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 cruzar la Internet pública.

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 VPCs, 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 final de administración de AWS cuentas en su VPC mediante Consola de administración de AWS, AWS Command Line Interface (AWS CLI), un AWS SDK, la API de administración de AWS cuentas o CloudFormation

Para obtener información sobre cómo crear y configurar un punto de conexión mediante la consola de Amazon VPC o la AWS CLI, consulte [Creación de un punto de conexión 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 final mediante CloudFormation, consulte el VPCEndpoint recurso [AWS: :EC2::](#) en la Guía del CloudFormation usuario.

Políticas de punto de conexión de VPC de Amazon

Puede controlar qué acciones se pueden realizar con este punto de conexión de servicio si adjunta una política de punto de conexión cuando crea el punto de conexión 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

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 en 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 quiere conceder acceso a las cuentas que forman parte de una AWS organización a un director que se encuentra 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 la administración de AWS cuentas

AWS Identity and Access Management (IAM) es un 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 un Servicio de AWS herramienta que puede utilizar sin coste adicional.

Temas

- [Público](#)
- [Autenticación con identidades](#)
- [Administración del acceso con políticas](#)
- [Cómo funciona AWS la administración de cuentas con IAM](#)
- [Ejemplos de políticas basadas en la identidad para la administración de cuentas AWS](#)
- [Uso de políticas basadas en la identidad \(políticas de IAM\) para la administración de cuentas AWS](#)
- [Solución de problemas AWS de identidad y acceso a la administración de cuentas](#)

Público

La forma de usar AWS Identity and Access Management (IAM) varía según la función que desempeñes:

- Usuario del servicio: solicite permisos al administrador si no puede acceder a las características (consulte [Solución de problemas AWS de identidad y acceso a la administración de cuentas](#)).
- Administrador del servicio: determine el acceso de los usuarios y envíe las solicitudes de permiso (consulte [Cómo funciona AWS la administración de cuentas con IAM](#)).
- Administrador de IAM: escribe las políticas para administrar el acceso (consulte [Ejemplos de políticas basadas en la identidad para la administración de cuentas AWS](#)).

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 root

Al crear un Cuenta de AWS, se comienza con una identidad de inicio de sesión denominada usuario Cuenta de AWS raíz que tiene acceso completo a todos Servicios de AWS los recursos. Se recomienda encarecidamente 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

El acceso se controla AWS creando políticas y adjuntándolas 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.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de política de permisos JSON que asocia 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.

Las políticas basadas en identidad pueden ser políticas insertadas (incrustadas 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.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de políticas JSON que se asocian 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.

Las políticas basadas en recursos son políticas insertadas 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 (SCPs): 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 (RCPs): establece los permisos máximos disponibles para los recursos de tus cuentas. Para obtener más información, consulte [Políticas de control de recursos \(RCPs\)](#) en la Guía del AWS Organizations usuario.
- 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 funciona AWS la administración de cuentas con IAM

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 puedes usar con AWS la administración de cuentas

Característica de IAM	Compatibilidad con Account Management
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política	Sí
ACLs	No
ABAC (etiquetas en políticas)	No
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	No
Roles vinculados al servicio	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](#).

Políticas basadas en identidades para Account Management

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. 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.

Ejemplos de políticas basadas en identidades para Account Management

Para ver ejemplos de políticas basadas en identidades de Account Management, consulte [Ejemplos de políticas basadas en la identidad para la administración de cuentas AWS](#).

Políticas basadas en recursos dentro de Account Management

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de política JSON que se asocian 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 directores 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 [Ejemplos de políticas basadas en la identidad para la administración de cuentas AWS](#).

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 `Resources` 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 respectivos tipos ARNs, 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 [Ejemplos de políticas basadas en la identidad para la administración de cuentas AWS](#).

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 [Ejemplos de políticas basadas en la identidad para la administración de cuentas AWS](#).

Listas de control de acceso en Account Management

Soportes ACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Control de acceso basado en atributos con Account Management

Compatibilidad con ABAC (etiquetas en las políticas): no

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de 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 mediante la clave de `account:AccountResourceOrgTags/key-name` condición. El espacio de nombres de la cuenta no admite la clave APIs de `aws:ResourceTag/key-name` condición estándar.

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 «» y el valor «12345» o «CostCenter67890» 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.

Permisos de entidades principales entre servicios para Account Management

Admite sesiones de acceso directo (FAS): sí

Las sesiones de acceso directo (FAS) utilizan los permisos del principal que llama y los que solicitan Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS 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.

Roles vinculados al servicio para Account Management

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 el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en su 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 Yes en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en la identidad para la administración de cuentas AWS

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 ARNs formato de cada uno de los tipos de recursos, consulte [Acciones, recursos y 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 el Consola de administración de AWS](#)
- [Proporcionar acceso completo a la página de la cuenta en el Consola de administración de AWS](#)

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan si alguien puede crear o eliminar los recursos de Account Management en la cuenta, como también acceder a ellos. 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` o la política `AWSAccountManagementReadOnlyAccess` 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 elegir permitir el acceso solo a las acciones que coincidan con las operaciones de API que intenta realizar.

Proporcionar acceso de solo lectura a la página de la cuenta en el 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 el 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 la administración de cuentas AWS

[Para obtener información completa sobre los usuarios de Cuentas de AWS 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 [Ejemplos de políticas basadas en la identidad para la administración de cuentas AWS](#).

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)
<code>account:ListRegions</code>	Enumeración	Concede permiso para enumerar las regiones disponibles.
<code>account:GetAccountInformation</code>	Lectura	Concede permiso para recuperar la información de una cuenta.
<code>account:GetAlternateContact</code>	Lectura	Concede permiso para recuperar los contactos alternativos de una cuenta.
<code>account:GetContactInformation</code>	Lectura	Concede permiso para recuperar la información de contacto principal de una cuenta.
<code>account:GetPrimaryEmail</code>	Lectura	Concede permiso para recuperar la dirección de correo electrónico principal de una cuenta.
<code>account:GetRegionOptStatus</code>	Lectura	Concede permiso para obtener el estado de suscripción de una región.
<code>account:AcceptPrimaryEmailUpdate</code>	Escritura	Otorga permiso para aceptar la actualización de la dirección de correo electrónico principal de la cuenta del miembro de una AWS organización.
<code>account:CloseAccount</code>	Escritura	Concede permiso para cerrar una cuenta.

Nombre del permiso	Nivel de acceso	Description (Descripción)
		 Note Este es un permiso solo para la consola. No hay acceso de API disponible para este permiso.
<code>account:DeleteAlternateContact</code>	Escritura	Concede permiso para eliminar los contactos alternativos de una cuenta.
<code>account:DisableRegion</code>	Escritura	Concede permiso para deshabilitar el uso de una región.
<code>account:EnableRegion</code>	Escritura	Concede permiso para habilitar el uso de una región.
<code>account:PutAccountName</code>	Escritura	Concede permiso para actualizar el nombre de una cuenta.
<code>account:PutAlternateContact</code>	Escritura	Concede permiso para modificar los contactos alternativos de una cuenta.
<code>account:PutContactInformation</code>	Escritura	Concede permiso para actualizar la información de contacto principal de una cuenta.

Nombre del permiso	Nivel de acceso	Description (Descripción)
<code>account:StartPrimaryEmailUpdate</code>	Escritura	Otorga permiso para iniciar la actualización de la dirección de correo electrónico principal de la cuenta del miembro de una AWS organización.

Solución de problemas AWS de identidad y acceso a la administración de cuentas

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 tengo autorización para realizar iam:PassRole](#)
- [Quiero permitir que personas ajenas a mí accedan Cuenta de AWS 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.



You Need Permissions

You don't have permission to access billing information for this account. Contact your AWS administrator if you need help. If you are an AWS administrator, you can provide permissions for your users or groups by making sure that (1) [this account allows IAM and federated users to access billing information](#) and (2) [you have the required IAM permissions](#).

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 tengo autorización para realizar `iam: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.

Algunos 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 mí accedan Cuenta de AWS 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 admiten políticas basadas en recursos o listas de control de acceso (ACLs), puedes usar esas políticas para permitir que las personas accedan a tus recursos.

Para obtener más información, consulte lo siguiente:

- Para obtener información acerca de si Account Management admite estas características, consulte [Cómo funciona AWS la administración de cuentas con IAM](#).

- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte [Proporcionar acceso a un usuario de IAM en otro de su propiedad en la Cuenta de AWS 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 gestionadas para la gestión de AWS cuentas

AWS La administración de cuentas ofrece actualmente dos políticas AWS administradas que están disponibles para su uso:

- [AWS política gestionada: AWSAccount ManagementReadOnlyAccess](#)
- [AWS política gestionada: AWSAccount ManagementFullAccess](#)
- [La administración de cuentas actualiza las políticas AWS administradas](#)

Una política AWS administrada 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 estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte [Políticas administradas por AWS](#) en la Guía del usuario de IAM.

AWS política gestionada: AWSAccount ManagementReadOnlyAccess

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 el Cuenta de AWS (solo puede ver el estado de las regiones de 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 habilitarla o deshabilitarla Regiones de AWS .

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: AWSAccount ManagementFullAccess

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 el Cuenta de AWS (solo puede ver el estado o habilitar o deshabilitar las regiones de su 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 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": "*"
    }
  ]
}
```

La administración de cuentas actualiza las políticas AWS 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	<p>La administración de cuentas se lanzó inicialmente con las siguientes AWS políticas de administración:</p> <ul style="list-style-type: none"> • AWSAccountManagemementReadOnlyAccess • AWSAccountManagemementFullAccess 	30 de septiembre de 2021

Validación de conformidad para la gestión de AWS cuentas

Los auditores externos evalúan la seguridad y el cumplimiento de AWS los servicios que puede ejecutar Cuenta de AWS 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 los programas de cumplimiento específicos, consulte [Servicios de AWS el ámbito por programa de cumplimiento Servicios de AWS](#) . Para obtener información general, consulte Programas de [AWS cumplimiento > Programas AWS](#) .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte [Descarga de informes en AWS Artifact](#) la Guía del AWS Artifact usuario.

Su responsabilidad en materia de cumplimiento al utilizar sus servicios Cuenta de AWS viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos 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.

- Diseño de [arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services](#): en este documento técnico se describe cómo pueden utilizar AWS las empresas para crear aplicaciones aptas para la HIPAA.

Note

No Servicios de AWS todas cumplen con los requisitos de la HIPAA. Para más información, consulte la [Referencia de servicios compatibles con HIPAA](#).

- [AWS Recursos de](#) cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- [Evaluación de los recursos con las reglas](#) de la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- [AWS Security Hub CSPM](#)— Este Servicio de AWS proporciona una visión integral del estado de su seguridad AWS que le ayuda a comprobar su conformidad con 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 la gestión de AWS cuentas

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 las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte [Infraestructura AWS global](#).

Seguridad de la infraestructura en AWS Account Management

Como servicios gestionados, AWS los servicios que se ejecutan en su Cuenta de AWS interior están protegidos por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS

de seguridad y cómo se AWS protege la infraestructura, consulte [Seguridad AWS en la nube](#). Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte [Protección de infraestructuras en un marco](#) de buena AWS arquitectura basado en el pilar de la seguridad.

Utiliza las llamadas a la API AWS publicadas 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 confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral 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.

Supervisa tu Cuenta de AWS

La supervisión es una parte importante del mantenimiento de la confiabilidad, la disponibilidad y el rendimiento de la administración de AWS cuentas y del resto de sus AWS soluciones. AWS proporciona las siguientes herramientas de supervisión para supervisar la gestión de las cuentas, informar cuando algo va mal y tomar medidas automáticas cuando sea necesario:

- AWS CloudTrail captura (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 un 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 una 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 de 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, consulta la [Guía del EventBridge usuario de Amazon](#).

Registro de llamadas a la API de administración de AWS cuentas mediante AWS CloudTrail

La administración de AWS cuentas APIs está integrada con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio que implica una operación de administración de cuentas. CloudTrail captura 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 una ruta, 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 configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por usted CloudTrail, puede determinar la solicitud que llevó a cabo una operación de administración de cuentas, la dirección IP utilizada para realizar la solicitud, quién la realizó y cuándo, así como detalles adicionales.

Para obtener más información CloudTrail, consulta la [Guía AWS CloudTrail del usuario](#).

Información sobre la administración de cuentas en CloudTrail

CloudTrail está activada en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una 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. Puede ver, buscar y descargar los eventos recientes en su Cuenta de AWS. Para obtener más información, consulte [Visualización de eventos con el historial de CloudTrail eventos](#).

Para tener un registro continuo de tus eventos Cuenta de AWS, incluidos los relacionados con las operaciones de administración de cuentas, crea un registro. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando crea una ruta en el Consola de administración de AWS, la ruta se aplica a todas 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 actuar en función de ellos. Para más información, consulte los siguientes temas:

- [Introducción a la creación de registros de seguimiento](#)
- [CloudTrail servicios e integraciones compatibles](#)
- [Configuración de 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 la API](#) de esta guía. Por ejemplo, las llamadas a las PutAlternateContact operaciones CreateAccountDeleteAlternateContact, y generan entradas en los archivos de CloudTrail registro.

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 root 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 realizó otro servicio AWS

Para obtener más información, consulte el [elemento userIdentity de CloudTrail](#).

Descripción de las entradas de registros de Account Management

Un rastro 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 solicitud única 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: En el siguiente ejemplo, se 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": "AROAI234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAI234567890EXAMPLE",
        "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 destinada a añadir un nuevo contacto BILLING alternativo a una cuenta.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAI234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAI234567890EXAMPLE",
        "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 para eliminar el contacto OPERATIONS alternativo actual.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "ARO1234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "ARO1234567890EXAMPLE",
        "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"
}
```

Supervisar los eventos de administración de cuentas con EventBridge

Amazon EventBridge, anteriormente denominado CloudWatch Events, le ayuda a supervisar los eventos que son específicos de otros e iniciar acciones segmentadas que utilizan otros Servicios de AWS. Los eventos de Servicios de AWS se envían EventBridge prácticamente en tiempo real.

Con EventBridge él, puede crear reglas que coincidan con los eventos entrantes y enviarlos a los objetivos para su procesamiento.

Para obtener más información, consulta [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 y deshabilitar las regiones y CloudTrail las llamadas a la API mediante regiones.

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 que realiza la 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 y: `GetRegionOptStatus` `ListRegions` APIs

- **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 ejemplo de patrón de eventos crea una regla que captura solo los eventos de la región **ENABLED** y **DISABLED**.

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

Solucione los problemas de su Cuenta de AWS

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 [Solucionar problemas de inicio de sesión en la Cuenta de AWS](#) en la Guía del usuario para el inicio de sesión en AWS .

Temas de solución de problemas

- [Solución de problemas relacionados con Cuenta de AWS la creación](#)
- [Solución de problemas relacionados con Cuenta de AWS el cierre](#)
- [Solución de otros problemas con Cuentas de AWS](#)

Solución de problemas relacionados con Cuenta de AWS la creación

Utilice los enlaces de referencia de la siguiente tabla para diagnosticar y solucionar problemas relacionados con la creación de una nueva Cuenta de AWS.

Problema	Enlace de referencia	origen
No sé cómo registrarme o crear una cuenta	Crea un Cuenta de AWS	Esta guía
¿Qué debo hacer si no he recibido ninguna 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 «número máximo de intentos fallidos» cuando intento verificarlo Cuenta de AWS por teléfono?	https://repost.aws/knowledge-center/maximum-intentos-fallidos	AWS re:Post

Problema	Enlace de referencia	origen
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 Guía del usuario para iniciar sesión

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 relacionados con Cuenta de AWS el cierre

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 un mensaje de error ConstraintViolationException «» al intentar cerrar mi cuenta](#)
- [Recibo el mensaje de error "CLOSE_ACCOUNT_QUOTA_EXCEEDED" cuando intento cerrar una cuenta de miembro](#)
- [¿Debo eliminar mi AWS 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. Debes [iniciar sesión Consola de administración de AWS como usuario root](#) para cerrar tu 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 root](#) 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 que el cierre se ha realizado correctamente comprobando 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 su organización, vaya a la AWS Organizations consola y asegúrese 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 un mensaje de error ConstraintViolationException «» al intentar cerrar mi cuenta

Está intentando cerrar una cuenta de administración mediante la AWS Organizations consola, lo cual 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 puede cerrar el 10 % de las cuentas de afiliados en un plazo de 30 días consecutivos. 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 cuenta del 10 %. El cierre mínimo es de 10 cuentas y el cierre máximo es de 1000 cuentas, incluso si el 10 % de las cuentas supera las 1000. Para obtener más información sobre las cuotas de Organizations, consulte [Quotas for AWS Organizations](#) en la Guía del usuario de AWS Organizations.

¿Debo eliminar mi AWS 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 su organización, vaya a la AWS Organizations consola y asegúrese de que todas las cuentas de los miembros aparezcan C*l*osed junto a sus nombres de cuenta. Después de eso, puede cerrar la cuenta de administración.

Solución de otros problemas con Cuentas de AWS

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 una Cuenta de AWS actividad fraudulenta](#)
- [Necesito cerrar mi Cuenta de AWS](#)

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 una Cuenta de AWS actividad fraudulenta

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 tiene problemas con una compra realizada en Amazon.com, consulte el [Servicio 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, consulta [Cerrar un Cuenta de AWS](#).

Cerrar un Cuenta de AWS

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 periodo comprendido entre el día en que usted cerró la cuenta y el momento en que AWS la cierra definitivamente se denomina [periodo 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, puede iniciar sesión y acceder a una Cuenta de AWS cerrada durante el [periodo posterior al cierre](#) solo para ver la información de facturación anterior, acceder a la configuración de la cuenta o ponerse en contacto con [AWS Support](#).
- 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 [Actualizar la dirección de correo electrónico del usuario raíz](#).

- 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 10 % de las cuentas de afiliados en un plazo de 30 días consecutivos. 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 cuenta del 10 %. El cierre mínimo es de 10 cuentas y el cierre máximo es de 1000 cuentas, incluso si el 10 % de las cuentas supera las 1000. 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](#).

- 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 relacionados con Cuenta de AWS el 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 ninguna operación de API de uno de los AWS SDKs. AWS CLI 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 la 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. Elija Close (Cerrar) 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 [Facturación unificada](#), no podrá ver el botón Cerrar de 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 step-by-step obtener orientación, sigue las instrucciones de la pestaña Cuenta independiente.

Para cerrar una cuenta de miembro mediante AWS CLI y SDKs

Para obtener instrucciones sobre cómo cerrar una cuenta de miembro mediante AWS CLI y SDKs, 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 C1osed 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 ninguna de las AWS SDKs. 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 relacionados con Cuenta de AWS el 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.

Periodo posterior al cierre

El período posterior al cierre se refiere al tiempo transcurrido entre el día en que cerraste tu cuenta y el momento en que la AWS cierras definitivamente. 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, (1) debe ponerse en contacto con [AWS Support](#) lo antes posible y (2) debemos recibir el pago total de cualquier saldo pendiente, incluida la información requerida tal 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 su cuenta se reiniciarán si la vuelve a abrir.

referencia de la API

Las operaciones de la API en el espacio de nombres de Account Management (account) le permiten modificar su. Cuenta de AWS

Every Cuenta de AWS admite metadatos con información sobre la cuenta, incluida información sobre hasta tres contactos alternativos asociados a la cuenta. Estos se suman a la dirección de correo electrónico asociada al [usuario raíz](#) de la cuenta. Puede especificar solo uno de los siguientes tipos de contacto asociados a una cuenta.

- Contacto de facturación
- Contacto de operaciones
- Contacto de seguridad

De forma predeterminada, las operaciones de la API que se describen en esta guía se aplican directamente a la cuenta que llama a la operación. La [identidad](#) en la cuenta que llama a la operación suele ser un rol de IAM o un usuario de IAM y debe tener el permiso aplicado por una política de IAM para llamar a la operación de API. Como alternativa, puedes llamar a estas operaciones de la API desde una identidad de una cuenta de AWS Organizations administración y especificar el número de ID de la cuenta de cualquiera Cuenta de AWS que sea miembro de la organización.

Versión de la API

Esta versión de la referencia de la API de cuentas registra la versión 2021-02-01 de la API de Account Management.

Note

Como alternativa a usar la API directamente, puede usar una de las AWS SDKs, que consta de bibliotecas y código de muestra para varios lenguajes de programación y plataformas (Java, Ruby, .NET, iOS, Android y más). SDKs Proporcionan una forma cómoda de crear un acceso programático a AWS Organizations. Por ejemplo, se SDKs encargan de firmar criptográficamente las solicitudes, gestionar los errores y volver a intentar las solicitudes automáticamente. Para obtener más información acerca de AWS SDKs, incluida la forma de descargarlos e instalarlos, consulte [Herramientas para Amazon Web Services](#).

Le recomendamos que lo utilice AWS SDKs para realizar llamadas programáticas a la API del servicio de administración de cuentas. Sin embargo, también puede usar la API de consulta de Account Management para realizar llamadas directas al servicio web de Account Management. Para obtener más información sobre la API de consultas de Account Management, consulte [Llamar a la API mediante solicitudes de consulta HTTP](#) en la Guía del usuario de Account Management. Organizations admite solicitudes GET y POST para todas las acciones. Es decir, la API no requiere que utilice GET para algunas acciones y POST para otras. Sin embargo, las solicitudes GET están sujetas a las limitaciones de tamaño de una URL. Por lo tanto, para las operaciones que requieran tamaños más grandes, utilice una solicitud POST.

Firma de solicitudes

Cuando envíes solicitudes HTTP a AWS, debes firmarlas para AWS poder identificar quién las envió. Las solicitudes se firman con la clave de AWS acceso, que consta de un identificador de clave de acceso y una clave de acceso secreta. Le recomendamos no crear una clave de acceso para su cuenta raíz. Cualquier persona que tenga la clave de acceso de su cuenta raíz dispondrá de acceso ilimitado a todos los recursos de su cuenta. En su lugar, cree una clave de acceso para un usuario de IAM que tenga privilegios de administrador. Otra opción es utilizar el AWS Security Token Service para generar credenciales de seguridad temporales y utilizarlas para firmar las solicitudes.

Para firmar solicitudes, le recomendamos que utilice la versión 4 de Signature. Si ya tiene una aplicación que utiliza la versión 2 de Signature, no tiene que actualizarla para utilizar la versión 4 de Signature. Sin embargo, algunas operaciones ahora requieren la versión 4 de Signature. En la documentación de las operaciones que requieren la versión 4, se indica este requisito. Para obtener más información, consulte [Firmar solicitudes de AWS API](#) en la Guía del usuario de IAM.

Cuando utiliza la interfaz de línea de AWS comandos (AWS CLI) o una de ellas AWS SDKs para realizar solicitudes AWS, estas herramientas firman automáticamente las solicitudes por usted con la clave de acceso que especifique al configurar las herramientas.

Compatibilidad con Account Management y comentarios

Agradecemos sus comentarios. Envíe sus comentarios a feedback-awsaccounts@amazon.com o publique sus comentarios y preguntas en el [foro de soporte de Account Management](#). Para obtener más información sobre los foros de AWS soporte, consulte la [Ayuda de los foros](#).

Cómo se presentan los ejemplos

El JSON devuelto por Account Management como respuesta a sus solicitudes se devuelve como una sola cadena larga sin saltos de línea ni espacios en blanco de formato. Tanto los saltos de línea

como los espacios en blanco se muestran en los ejemplos de esta guía para mejorar la legibilidad. Si los parámetros de entrada de ejemplo también dan como resultado cadenas largas que se extienden más allá de la pantalla, insertamos saltos de línea para mejorar la legibilidad. Siempre debe enviar la entrada como una sola cadena de texto JSON.

Registro de solicitudes de API

Account Management admite CloudTrail un servicio que registra sus llamadas a la AWS API Cuenta de AWS y entrega los archivos de registro a un bucket de Amazon S3. Al usar la información recopilada por CloudTrail, puede determinar qué solicitudes se realizaron correctamente a la administración de cuentas, quién realizó la solicitud, cuándo se realizó, etc. Para obtener más información sobre la administración de cuentas y su soporte CloudTrail, consulte [Registro de llamadas a la API de administración de AWS cuentas mediante AWS CloudTrail](#). Para obtener más información sobre CloudTrail cómo activarla y buscar los archivos de registro, consulta la [Guía del AWS CloudTrail usuario](#).

Acciones

Se admiten las siguientes acciones:

- [AcceptPrimaryEmailUpdate](#)
- [DeleteAlternateContact](#)
- [DisableRegion](#)
- [EnableRegion](#)
- [GetAccountInformation](#)
- [GetAlternateContact](#)
- [GetContactInformation](#)
- [GetGovCloudAccountInformation](#)
- [GetPrimaryEmail](#)
- [GetRegionOptStatus](#)
- [ListRegions](#)
- [PutAccountName](#)
- [PutAlternateContact](#)
- [PutContactInformation](#)
- [StartPrimaryEmailUpdate](#)

AcceptPrimaryEmailUpdate

Acepta la solicitud originada por [StartPrimaryEmailUpdate](#) para actualizar la dirección de correo electrónico principal (también conocida como dirección de correo electrónico del usuario raíz) de la cuenta especificada.

Sintaxis de la solicitud

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

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

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

AccountId

Especifica el número de ID de cuenta de 12 dígitos al Cuenta de AWS que desea acceder o modificar con esta operación. Para usar este parámetro, la persona que llama debe ser una identidad de la [cuenta de administración de la organización](#) o una cuenta de administrador delegado. El ID de cuenta especificado debe ser una cuenta de miembro en la misma organización. La organización debe tener [todas las características habilitadas](#), así como el [acceso de confianza](#) habilitado para el servicio de Account Management y, de manera opcional, puede tener asignada una cuenta de [administrador delegado](#).

Esta operación solo se puede realizar desde la cuenta de administración o desde la cuenta de administrador delegado de una organización para una cuenta de miembro.

Note

La cuenta de administración no puede especificar su propio AccountId.

Tipo: cadena

Patrón: \d{12}

Obligatorio: sí

Otp

El código OTP enviado al `PrimaryEmail` especificada en la llamada a la API `StartPrimaryEmailUpdate`.

Tipo: cadena

Patrón: [a-zA-Z0-9]{6}

Obligatorio: sí

PrimaryEmail

La dirección de correo electrónico principal para la cuenta especificada. Debe coincidir con la `PrimaryEmail` de la llamada a la API `StartPrimaryEmailUpdate`.

Tipo: cadena

Restricciones de longitud: longitud mínima de 5 caracteres. La longitud máxima es de 64.

Obligatorio: sí

Sintaxis de la respuesta

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

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

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

Status

Recupera el estado de la solicitud de actualización del correo electrónico principal aceptada.

Tipo: cadena

Valores válidos: PENDING | ACCEPTED

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AccessDeniedException

Se ha producido un error en la operación porque la identidad que ha realizado la llamada no tiene los permisos mínimos necesarios.

errorType

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 403

ConflictException

No se pudo procesar la solicitud debido a un conflicto en el estado actual del recurso. Esto ocurre, por ejemplo, si intenta activar una región que está deshabilitada actualmente (en estado EN PROCESO DE DESHABILITACIÓN) o si intenta cambiar el correo electrónico del usuario raíz de una cuenta por una dirección de correo electrónico que ya esté en uso.

errorType

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 409

InternalServerErrorException

La operación falló debido a un error interno de AWS. Intente realizar la operación otra vez más tarde.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 500

ResourceNotFoundException

Se ha producido un error en la operación porque se ha especificado un recurso que no se encuentra.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 404

TooManyRequestsException

Se ha producido un error en la operación porque se la ha llamado con demasiada frecuencia y ha superado la limitación.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 429

ValidationException

Se ha producido un error en la operación porque uno de los parámetros de entrada no era válido.

`fieldList`

El campo en el que se detectó la entrada no válida.

`message`

El mensaje donde se le informa qué no era válido en la solicitud.

`reason`

El motivo por el que se produjo un error en la validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET V4](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DeleteAlternateContact

Elimina el contacto alternativo especificado de un Cuenta de AWS.

Para obtener detalles sobre cómo utilizar las operaciones de contacto alternativo, consulte [Actualizar los contactos alternativos para su Cuenta de AWS](#).

Note

Antes de poder actualizar la información de contacto alternativa de una Cuenta de AWS empresa gestionada por AWS Organizations, primero debe habilitar la integración entre AWS Account Management y Organizations. Para obtener más información, consulte [Habilitación del acceso de confianza para la administración de la cuenta de AWS](#).

Sintaxis de la solicitud

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

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

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud


La solicitud acepta los siguientes datos en formato JSON.

AccountId

Especifica el número de ID de cuenta de 12 dígitos de la AWS cuenta a la que desea acceder o modificar con esta operación.

Si no especifica este parámetro, el valor predeterminado será la AWS cuenta de la identidad utilizada para llamar a la operación.

Para usar este parámetro, la persona que llama debe ser una identidad de la [cuenta de administración de la organización](#) o una cuenta de administrador delegado, y el ID de cuenta especificado debe ser una cuenta de miembro en la misma organización. La organización debe tener [todas las características habilitadas](#), así como el [acceso de confianza](#) habilitado para el servicio de administración de cuentas y, de manera opcional, puede tener asignada una cuenta de [administrador delegado](#).

 Note

La cuenta de administración no puede especificar su propio AccountId; debe llamar a la operación en un contexto independiente al no incluir el parámetro AccountId.

Para llamar a esta operación en una cuenta que no es miembro de una organización, no especifique este parámetro y llame a la operación con una identidad que pertenezca a la cuenta cuyos contactos desea recuperar o modificar.

Tipo: cadena

Patrón: `\d{12}`

Obligatorio: no

[AlternateContactType](#)

Especifica cuáles de los contactos alternativos se van a eliminar.

Tipo: cadena

Valores válidos: BILLING | OPERATIONS | SECURITY

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AccessDeniedException

Se ha producido un error en la operación porque la identidad que ha realizado la llamada no tiene los permisos mínimos necesarios.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 403

InternalServerErrorException

La operación falló debido a un error interno de AWS. Intente realizar la operación otra vez más tarde.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 500

ResourceNotFoundException

Se ha producido un error en la operación porque se ha especificado un recurso que no se encuentra.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 404

TooManyRequestsException

Se ha producido un error en la operación porque se la ha llamado con demasiada frecuencia y ha superado la limitación.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 429

ValidationException

Se ha producido un error en la operación porque uno de los parámetros de entrada no era válido.

fieldList

El campo en el que se detectó la entrada no válida.

message

El mensaje donde se le informa qué no era válido en la solicitud.

reason

El motivo por el que se produjo un error en la validación.

Código de estado HTTP: 400

Ejemplos

Ejemplo 1

En el siguiente ejemplo, se elimina el contacto alternativo de seguridad de la cuenta cuyas credenciales se utilizan para llamar a la operación.

Solicitud de muestra

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

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

Respuesta de ejemplo

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

Ejemplo 2

En el siguiente ejemplo, se elimina el contacto alternativo de facturación de la cuenta de miembro especificada en una organización. Debe usar las credenciales de la cuenta de administración de la organización o de la cuenta de administrador delegado del servicio de Account Management.

Solicitud de muestra

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

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

Respuesta de ejemplo

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

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET V4](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DisableRegion

Deshabilita (excluye) una región determinada de una cuenta.

Note

La deshabilitación de una región eliminará todo acceso de IAM a cualquier recurso que resida en esa región.

Sintaxis de la solicitud

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

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

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

AccountId

Especifica el número de ID de cuenta de 12 dígitos al Cuenta de AWS que desea acceder o modificar con esta operación. Si no especifica este parámetro, el valor predeterminado será la cuenta de Amazon Web Services de la identidad utilizada para llamar a la operación. Para usar este parámetro, la persona que llama debe ser una identidad de la [cuenta de administración de la organización](#) o una cuenta de administrador delegado. El ID de cuenta especificado debe ser una cuenta de miembro en la misma organización. La organización debe tener [todas las características habilitadas](#), así como el [acceso de confianza](#) habilitado para el servicio de Account Management y, de manera opcional, puede tener asignada una cuenta de [administrador delegado](#).

Note

La cuenta de administración no puede especificar su propio AccountId. Debe llamar a la operación en un contexto independiente al no incluir el parámetro AccountId.

Para llamar a esta operación en una cuenta que no es miembro de una organización, no especifique este parámetro. En su lugar, llame a la operación con una identidad que pertenezca a la cuenta cuyos contactos desea recuperar o modificar.

Tipo: cadena

Patrón: `\d{12}`

Obligatorio: no

RegionName

Especifica el código de región de un nombre de región determinado (por ejemplo, `af-south-1`). Al deshabilitar una región, AWS realiza acciones para desactivarla en su cuenta, como destruir los recursos de IAM de la región. Este proceso tarda unos minutos para la mayoría de las cuentas, pero puede tardar varias horas. No puede habilitar la región hasta que el proceso de deshabilitación se haya realizado por completo.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 50 caracteres.

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AccessDeniedException

Se ha producido un error en la operación porque la identidad que ha realizado la llamada no tiene los permisos mínimos necesarios.

errorType

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 403

ConflictException

No se pudo procesar la solicitud debido a un conflicto en el estado actual del recurso. Esto ocurre, por ejemplo, si intenta activar una región que está deshabilitada actualmente (en estado EN PROCESO DE DESHABILITACIÓN) o si intenta cambiar el correo electrónico del usuario raíz de una cuenta por una dirección de correo electrónico que ya esté en uso.

errorType

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 409

InternalServerError

La operación falló debido a un error interno de AWS. Intente realizar la operación otra vez más tarde.

errorType

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 500

TooManyRequestsException

Se ha producido un error en la operación porque se la ha llamado con demasiada frecuencia y ha superado la limitación.

errorType

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 429

ValidationException

Se ha producido un error en la operación porque uno de los parámetros de entrada no era válido.

fieldList

El campo en el que se detectó la entrada no válida.

message

El mensaje donde se le informa qué no era válido en la solicitud.

reason

El motivo por el que se produjo un error en la validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET V4](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

EnableRegion

Habilita (suscribe) una región en particular para una cuenta.

Sintaxis de la solicitud

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

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

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

AccountId

Especifica el número de ID de cuenta de 12 dígitos al Cuenta de AWS que desea acceder o modificar con esta operación. Si no especifica este parámetro, el valor predeterminado será la cuenta de Amazon Web Services de la identidad utilizada para llamar a la operación. Para usar este parámetro, la persona que llama debe ser una identidad de la [cuenta de administración de la organización](#) o una cuenta de administrador delegado. El ID de cuenta especificado debe ser una cuenta de miembro en la misma organización. La organización debe tener [todas las características habilitadas](#), así como el [acceso de confianza](#) habilitado para el servicio de Account Management y, de manera opcional, puede tener asignada una cuenta de [administrador delegado](#).

Note

La cuenta de administración no puede especificar su propio AccountId. Debe llamar a la operación en un contexto independiente al no incluir el parámetro AccountId.

Para llamar a esta operación en una cuenta que no es miembro de una organización, no especifique este parámetro. En su lugar, llame a la operación con una identidad que pertenezca a la cuenta cuyos contactos desea recuperar o modificar.

Tipo: cadena

Patrón: `\d{12}`

Obligatorio: no

RegionName

Especifica el código de región de un nombre de región determinado (por ejemplo, `af-south-1`). Al activar 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 puede tardar varias horas. No puede utilizar la región hasta que este proceso finalice. Además, no puede deshabilitar la región hasta que el proceso de habilitación se haya realizado por completo.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 50 caracteres.

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AccessDeniedException

Se ha producido un error en la operación porque la identidad que ha realizado la llamada no tiene los permisos mínimos necesarios.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 403

ConflictException

No se pudo procesar la solicitud debido a un conflicto en el estado actual del recurso. Esto ocurre, por ejemplo, si intenta activar una región que está deshabilitada actualmente (en estado EN PROCESO DE DESHABILITACIÓN) o si intenta cambiar el correo electrónico del usuario raíz de una cuenta por una dirección de correo electrónico que ya esté en uso.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 409

InternalServerErrorException

La operación falló debido a un error interno de AWS. Intente realizar la operación otra vez más tarde.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 500

TooManyRequestsException

Se ha producido un error en la operación porque se la ha llamado con demasiada frecuencia y ha superado la limitación.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 429

ValidationException

Se ha producido un error en la operación porque uno de los parámetros de entrada no era válido.

`fieldList`

El campo en el que se detectó la entrada no válida.

`message`

El mensaje donde se le informa qué no era válido en la solicitud.

`reason`

El motivo por el que se produjo un error en la validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET V4](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

GetAccountInformation

Recupera información sobre la cuenta especificada, incluidos el nombre, el identificador y la fecha y hora de creación de la cuenta. Para usar esta API, un rol o usuario de IAM deben tener el permiso de `account:GetAccountInformation` IAM.

Sintaxis de la solicitud

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

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

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

AccountId

Especifica el número de ID de cuenta de 12 dígitos de la AWS cuenta a la que desea acceder o modificar con esta operación.

Si no especifica este parámetro, el valor predeterminado será la AWS cuenta de la identidad utilizada para llamar a la operación.

Para usar este parámetro, la persona que llama debe ser una identidad de la [cuenta de administración de la organización](#) o una cuenta de administrador delegado, y el ID de cuenta especificado debe ser una cuenta de miembro en la misma organización. La organización debe tener [todas las características habilitadas](#), así como el [acceso de confianza](#) habilitado para el servicio de administración de cuentas y, de manera opcional, puede tener asignada una cuenta de [administrador delegado](#).

Note

La cuenta de administración no puede especificar su propio AccountId; debe llamar a la operación en un contexto independiente al no incluir el parámetro AccountId.

Para llamar a esta operación en una cuenta que no es miembro de una organización, no especifique este parámetro y llame a la operación con una identidad que pertenezca a la cuenta cuyos contactos desea recuperar o modificar.

Tipo: cadena

Patrón: \d{12}

Obligatorio: no

Sintaxis de la respuesta

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

{
  "AccountCreatedDate": "string",
  "AccountId": "string",
  "AccountName": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

AccountCreatedDate

La fecha y hora de creación de la cuenta.

Tipo: marca temporal

AccountId

Especifica el número de ID de cuenta de 12 dígitos a la Cuenta de AWS que desea acceder o modificar con esta operación. Para usar este parámetro, la persona que llama debe ser una identidad de la [cuenta de administración de la organización](#) o una cuenta de administrador delegado. El ID de cuenta especificado debe ser una cuenta de miembro en la misma organización. La organización debe tener [todas las características habilitadas](#), así como el [acceso de confianza](#) habilitado para el servicio de Account Management y, de manera opcional, puede tener asignada una cuenta de [administrador delegado](#).

Esta operación solo se puede realizar desde la cuenta de administración o desde la cuenta de administrador delegado de una organización para una cuenta de miembro.

Note

La cuenta de administración no puede especificar su propio AccountId.

Tipo: cadena

Patrón: `\d{12}`

AccountName

El nombre de la cuenta.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 50 caracteres.

Patrón: `[- ; = ? - ~] +`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AccessDeniedException

Se ha producido un error en la operación porque la identidad que ha realizado la llamada no tiene los permisos mínimos necesarios.

errorType

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 403

InternalServerError

Se produjo un error en la operación debido a AWS un error interno. Intente realizar la operación otra vez más tarde.

errorType

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 500

TooManyRequestsException

Se ha producido un error en la operación porque se la ha llamado con demasiada frecuencia y ha superado la limitación.

errorType

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 429

ValidationException

Se ha producido un error en la operación porque uno de los parámetros de entrada no era válido.

fieldList

El campo en el que se detectó la entrada no válida.

message

El mensaje donde se le informa qué no era válido en la solicitud.

reason

El motivo por el que se produjo un error en la validación.

Código de estado HTTP: 400

Ejemplos

Ejemplo 1

En el siguiente ejemplo, se recupera la información de cuenta de la cuenta cuyas credenciales se utilizan para llamar a la operación.

Solicitud de muestra

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

{}
```

Respuesta de ejemplo

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

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

Ejemplo 2

En el siguiente ejemplo, se recupera la información de cuenta de la cuenta de miembro especificada en una organización. Debe usar las credenciales de la cuenta de administración de la organización o de la cuenta de administrador delegado del servicio de Account Management.

Solicitud de muestra

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

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

Respuesta de ejemplo

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

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

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET V4](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

GetAlternateContact

Recupera el contacto alternativo especificado adjunto a un Cuenta de AWS.

Para obtener detalles sobre cómo utilizar las operaciones de contacto alternativo, consulte [Actualizar los contactos alternativos para su Cuenta de AWS](#).

Note

Antes de poder actualizar la información de contacto alternativa de una Cuenta de AWS empresa gestionada por AWS Organizations, primero debe habilitar la integración entre AWS Account Management y Organizations. Para obtener más información, consulte [Habilitación del acceso de confianza para la administración de la cuenta de AWS](#).

Sintaxis de la solicitud

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

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

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud


La solicitud acepta los siguientes datos en formato JSON.

AccountId

Especifica el número de ID de cuenta de 12 dígitos de la AWS cuenta a la que desea acceder o modificar con esta operación.

Si no especifica este parámetro, el valor predeterminado será la AWS cuenta de la identidad utilizada para llamar a la operación.

Para usar este parámetro, la persona que llama debe ser una identidad de la [cuenta de administración de la organización](#) o una cuenta de administrador delegado, y el ID de cuenta especificado debe ser una cuenta de miembro en la misma organización. La organización debe tener [todas las características habilitadas](#), así como el [acceso de confianza](#) habilitado para el servicio de administración de cuentas y, de manera opcional, puede tener asignada una cuenta de [administrador delegado](#).

 Note

La cuenta de administración no puede especificar su propio AccountId; debe llamar a la operación en un contexto independiente al no incluir el parámetro AccountId.

Para llamar a esta operación en una cuenta que no es miembro de una organización, no especifique este parámetro y llame a la operación con una identidad que pertenezca a la cuenta cuyos contactos desea recuperar o modificar.

Tipo: cadena

Patrón: \d{12}

Obligatorio: no

[AlternateContactType](#)

Especifica qué contacto alternativo desea recuperar.

Tipo: cadena

Valores válidos: BILLING | OPERATIONS | SECURITY

Obligatorio: sí

Sintaxis de la respuesta

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

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

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

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[AlternateContact](#)

Una estructura que contiene los detalles del contacto alternativo especificado.

Tipo: objeto [AlternateContact](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AccessDeniedException

Se ha producido un error en la operación porque la identidad que ha realizado la llamada no tiene los permisos mínimos necesarios.

errorType

El valor que API Gateway rellena en el encabezado de respuesta de x-amzn-ErrorType.

Código de estado HTTP: 403

InternalServerError

La operación falló debido a un error interno de AWS. Intente realizar la operación otra vez más tarde.

errorType

El valor que API Gateway rellena en el encabezado de respuesta de x-amzn-ErrorType.

Código de estado HTTP: 500

ResourceNotFoundException

Se ha producido un error en la operación porque se ha especificado un recurso que no se encuentra.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 404

TooManyRequestsException

Se ha producido un error en la operación porque se la ha llamado con demasiada frecuencia y ha superado la limitación.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 429

ValidationException

Se ha producido un error en la operación porque uno de los parámetros de entrada no era válido.

`fieldList`

El campo en el que se detectó la entrada no válida.

`message`

El mensaje donde se le informa qué no era válido en la solicitud.

`reason`

El motivo por el que se produjo un error en la validación.

Código de estado HTTP: 400

Ejemplos

Ejemplo 1

En el siguiente ejemplo, se recupera el contacto alternativo de seguridad de la cuenta cuyas credenciales se utilizan para llamar a la operación.

Solicitud de muestra

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

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

Respuesta de ejemplo

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

{
  "AlternateContact": {
    "Name": "Anika",
    "Title": "C00",
    "EmailAddress": "anika@example.com",
    "PhoneNumber": "206-555-0198",
    "AlternateContactType": "Security"
  }
}
```

Ejemplo 2

En el siguiente ejemplo, se recupera el contacto alternativo de operaciones para la cuenta de miembro especificada en una organización. Debe usar las credenciales de la cuenta de administración de la organización o de la cuenta de administrador delegado del servicio de Account Management.

Solicitud de muestra

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

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

Respuesta de ejemplo

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

{
  "AlternateContact":{
    "Name":"Anika",
    "Title":"COO",
    "EmailAddress":"anika@example.com",
    "PhoneNumber":"206-555-0198",
    "AlternateContactType":"Operations"
  }
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET V4](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

GetContactInformation

Recupera la información de contacto principal de una Cuenta de AWS.

Para obtener detalles sobre cómo utilizar las operaciones de contacto principal, consulte [Actualizar el contacto principal para su Cuenta de AWS](#).

Sintaxis de la solicitud

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

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

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[AccountId](#)

Especifica el número de ID de cuenta de 12 dígitos al Cuenta de AWS que desea acceder o modificar con esta operación. Si no especifica este parámetro, el valor predeterminado será la cuenta de Amazon Web Services de la identidad utilizada para llamar a la operación. Para usar este parámetro, la persona que llama debe ser una identidad de la [cuenta de administración de la organización](#) o una cuenta de administrador delegado. El ID de cuenta especificado debe ser una cuenta de miembro en la misma organización. La organización debe tener [todas las características habilitadas](#), así como el [acceso de confianza](#) habilitado para el servicio de Account Management y, de manera opcional, puede tener asignada una cuenta de [administrador delegado](#).

Note

La cuenta de administración no puede especificar su propio AccountId. Debe llamar a la operación en un contexto independiente al no incluir el parámetro AccountId.

Para llamar a esta operación en una cuenta que no es miembro de una organización, no especifique este parámetro. En su lugar, llame a la operación con una identidad que pertenezca a la cuenta cuyos contactos desea recuperar o modificar.

Tipo: cadena

Patrón: \d{12}

Obligatorio: no

Sintaxis de la respuesta

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

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

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

ContactInformation

Contiene los detalles de la información de contacto principal asociada a una Cuenta de AWS.

Tipo: objeto [ContactInformation](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AccessDeniedException

Se ha producido un error en la operación porque la identidad que ha realizado la llamada no tiene los permisos mínimos necesarios.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 403

InternalServerError

La operación falló debido a un error interno de AWS. Intente realizar la operación otra vez más tarde.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 500

ResourceNotFoundException

Se ha producido un error en la operación porque se ha especificado un recurso que no se encuentra.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 404

TooManyRequestsException

Se ha producido un error en la operación porque se la ha llamado con demasiada frecuencia y ha superado la limitación.

errorType

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 429

ValidationException

Se ha producido un error en la operación porque uno de los parámetros de entrada no era válido.

fieldList

El campo en el que se detectó la entrada no válida.

message

El mensaje donde se le informa qué no era válido en la solicitud.

reason

El motivo por el que se produjo un error en la validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET V4](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

GetGovCloudAccountInformation

Recupera información sobre la GovCloud cuenta vinculada a la cuenta estándar especificada (si existe), incluidos el ID y el estado de la GovCloud cuenta. Para usar esta API, un rol o usuario de IAM deben tener el permiso de `account:GetGovCloudAccountInformation` IAM.

Sintaxis de la solicitud

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

{
  "StandardAccountId": "string"
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

StandardAccountId

Especifica el número de ID de cuenta de 12 dígitos de la AWS cuenta a la que desea acceder o modificar con esta operación.

Si no especifica este parámetro, el valor predeterminado será la AWS cuenta de la identidad utilizada para llamar a la operación.

Para usar este parámetro, la persona que llama debe ser una identidad de la [cuenta de administración de la organización](#) o una cuenta de administrador delegado, y el ID de cuenta especificado debe ser una cuenta de miembro en la misma organización. La organización debe tener [todas las características habilitadas](#), así como el [acceso de confianza](#) habilitado para el servicio de administración de cuentas y, de manera opcional, puede tener asignada una cuenta de [administrador delegado](#).

Note

La cuenta de administración no puede especificar su propio AccountId; debe llamar a la operación en un contexto independiente al no incluir el parámetro AccountId.

Para llamar a esta operación en una cuenta que no es miembro de una organización, no especifique este parámetro y llame a la operación con una identidad que pertenezca a la cuenta cuyos contactos desea recuperar o modificar.

Tipo: cadena

Patrón: \d{12}

Obligatorio: no

Sintaxis de la respuesta

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

{
  "AccountState": "string",
  "GovCloudAccountId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

AccountState

El estado de la GovCloud cuenta vinculada.

Tipo: cadena

Valores válidos: PENDING_ACTIVATION | ACTIVE | SUSPENDED | CLOSED

GovCloudAccountId

El número de identificación de cuenta de 12 dígitos de la GovCloud cuenta vinculada.

Tipo: cadena

Patrón: `\d{12}`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AccessDeniedException

Se ha producido un error en la operación porque la identidad que ha realizado la llamada no tiene los permisos mínimos necesarios.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 403

InternalServerError

La operación falló debido a un error interno de AWS. Intente realizar la operación otra vez más tarde.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 500

ResourceNotFoundException

Se ha producido un error en la operación porque se ha especificado un recurso que no se encuentra.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 404

ResourceUnavailableException

Se produjo un error en la operación porque especificó un recurso que no está disponible actualmente.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 424

TooManyRequestsException

Se ha producido un error en la operación porque se la ha llamado con demasiada frecuencia y ha superado la limitación.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 429

ValidationException

Se ha producido un error en la operación porque uno de los parámetros de entrada no era válido.

`fieldList`

El campo en el que se detectó la entrada no válida.

`message`

El mensaje donde se le informa qué no era válido en la solicitud.

`reason`

El motivo por el que se produjo un error en la validación.

Código de estado HTTP: 400

Ejemplos

Ejemplo 1

En el siguiente ejemplo, se recupera la información de la GovCloud cuenta vinculada cuyas credenciales se utilizan para llamar a la operación.

Solicitud de muestra

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

{}
```

Respuesta de ejemplo

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

{
  "GovCloudAccountId": "123456789012",
  "AccountState": "ACTIVE"
}
```

Ejemplo 2

El siguiente ejemplo recupera la información de la GovCloud cuenta vinculada de la cuenta de miembro especificada en una organización. Debe usar las credenciales de la cuenta de administración de la organización o de la cuenta de administrador delegado del servicio de Account Management.

Solicitud de muestra

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

{
  "StandardAccountId": "111111111111"
}
```

Respuesta de ejemplo

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

{
  "GovCloudAccountId": "123456789012",
  "AccountState": "ACTIVE"
}
```

```
}
```

Ejemplo 3

En el siguiente ejemplo, se intenta recuperar la información de la GovCloud cuenta vinculada de una cuenta estándar que no está vinculada a ninguna GovCloud cuenta.

Solicitud de muestra

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

{
  "StandardAccountId": "222222222222"
}
```

Respuesta de ejemplo

```
HTTP/1.1 404
Content-Type: application/json

{
  "message": "GovCloud Account ID not found for Standard Account - 222222222222."
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET V4](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)

- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

GetPrimaryEmail

Recupera la dirección de correo electrónico principal para la cuenta especificada.

Sintaxis de la solicitud

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

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

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

AccountId

Especifica el número de ID de cuenta de 12 dígitos al Cuenta de AWS que desea acceder o modificar con esta operación. Para usar este parámetro, la persona que llama debe ser una identidad de la [cuenta de administración de la organización](#) o una cuenta de administrador delegado. El ID de cuenta especificado debe ser una cuenta de miembro en la misma organización. La organización debe tener [todas las características habilitadas](#), así como el [acceso de confianza](#) habilitado para el servicio de Account Management y, de manera opcional, puede tener asignada una cuenta de [administrador delegado](#).

Esta operación solo se puede realizar desde la cuenta de administración o desde la cuenta de administrador delegado de una organización para una cuenta de miembro.

Note

La cuenta de administración no puede especificar su propio AccountId.

Tipo: cadena

Patrón: \d{12}

Obligatorio: sí

Sintaxis de la respuesta

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

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

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

PrimaryEmail

Recupera la dirección de correo electrónico principal asociada a la cuenta especificada.

Tipo: cadena

Restricciones de longitud: longitud mínima de 5 caracteres. La longitud máxima es de 64.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AccessDeniedException

Se ha producido un error en la operación porque la identidad que ha realizado la llamada no tiene los permisos mínimos necesarios.

errorType

El valor que API Gateway rellena en el encabezado de respuesta de x-amzn-ErrorType.

Código de estado HTTP: 403

InternalServerErrorException

La operación falló debido a un error interno de AWS. Intente realizar la operación otra vez más tarde.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 500

ResourceNotFoundException

Se ha producido un error en la operación porque se ha especificado un recurso que no se encuentra.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 404

TooManyRequestsException

Se ha producido un error en la operación porque se la ha llamado con demasiada frecuencia y ha superado la limitación.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 429

ValidationException

Se ha producido un error en la operación porque uno de los parámetros de entrada no era válido.

`fieldList`

El campo en el que se detectó la entrada no válida.

`message`

El mensaje donde se le informa qué no era válido en la solicitud.

`reason`

El motivo por el que se produjo un error en la validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET V4](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

GetRegionOptStatus

Recupera el estado de suscripción de una región determinada.

Sintaxis de la solicitud

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

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

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

AccountId

Especifica el número de ID de cuenta de 12 dígitos al Cuenta de AWS que desea acceder o modificar con esta operación. Si no especifica este parámetro, el valor predeterminado será la cuenta de Amazon Web Services de la identidad utilizada para llamar a la operación. Para usar este parámetro, la persona que llama debe ser una identidad de la [cuenta de administración de la organización](#) o una cuenta de administrador delegado. El ID de cuenta especificado debe ser una cuenta de miembro en la misma organización. La organización debe tener [todas las características habilitadas](#), así como el [acceso de confianza](#) habilitado para el servicio de Account Management y, de manera opcional, puede tener asignada una cuenta de [administrador delegado](#).

Note

La cuenta de administración no puede especificar su propio AccountId. Debe llamar a la operación en un contexto independiente al no incluir el parámetro AccountId.

Para llamar a esta operación en una cuenta que no es miembro de una organización, no especifique este parámetro. En su lugar, llame a la operación con una identidad que pertenezca a la cuenta cuyos contactos desea recuperar o modificar.

Tipo: cadena

Patrón: `\d{12}`

Obligatorio: no

RegionName

Especifica el código de región de un nombre de región determinado (por ejemplo, `af-south-1`). Esta función devolverá el estado de cualquier región que introduzca en este parámetro.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 50 caracteres.

Obligatorio: sí

Sintaxis de la respuesta

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

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

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

RegionName

El código de región que se introdujo.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 50 caracteres.

RegionOptStatus

Uno de los posibles estados que puede alcanzar una región (Habilitada, En proceso de habilitación, Deshabilitada, En proceso de deshabilitación, Habilitada por defecto).

Tipo: cadena

Valores válidos: ENABLED | ENABLING | DISABLING | DISABLED |
ENABLED_BY_DEFAULT

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AccessDeniedException

Se ha producido un error en la operación porque la identidad que ha realizado la llamada no tiene los permisos mínimos necesarios.

errorType

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 403

InternalServerError

La operación falló debido a un error interno de AWS. Intente realizar la operación otra vez más tarde.

errorType

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 500

TooManyRequestsException

Se ha producido un error en la operación porque se la ha llamado con demasiada frecuencia y ha superado la limitación.

errorType

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 429

ValidationException

Se ha producido un error en la operación porque uno de los parámetros de entrada no era válido.

fieldList

El campo en el que se detectó la entrada no válida.

message

El mensaje donde se le informa qué no era válido en la solicitud.

reason

El motivo por el que se produjo un error en la validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET V4](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ListRegions

Muestra todas las regiones de una cuenta determinada y sus respectivos estados de suscripción. Opcionalmente, esta lista se puede filtrar por el parámetro `region-opt-status-contains`.

Sintaxis de la solicitud

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

{
  "AccountId": "string",
  "MaxResults": number,
  "NextToken": "string",
  "RegionOptStatusContains": [ "string" ]
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

AccountId

Especifica el número de ID de cuenta de 12 dígitos al Cuenta de AWS que desea acceder o modificar con esta operación. Si no especifica este parámetro, el valor predeterminado será la cuenta de Amazon Web Services de la identidad utilizada para llamar a la operación. Para usar este parámetro, la persona que llama debe ser una identidad de la [cuenta de administración de la organización](#) o una cuenta de administrador delegado. El ID de cuenta especificado debe ser una cuenta de miembro en la misma organización. La organización debe tener [todas las características habilitadas](#), así como el [acceso de confianza](#) habilitado para el servicio de Account Management y, de manera opcional, puede tener asignada una cuenta de [administrador delegado](#).

Note

La cuenta de administración no puede especificar su propio AccountId. Debe llamar a la operación en un contexto independiente al no incluir el parámetro AccountId.

Para llamar a esta operación en una cuenta que no es miembro de una organización, no especifique este parámetro. En su lugar, llame a la operación con una identidad que pertenezca a la cuenta cuyos contactos desea recuperar o modificar.

Tipo: cadena

Patrón: `\d{12}`

Obligatorio: no

MaxResults

El número total de elementos que se devuelven en la salida del comando. Si el número total de elementos disponible es mayor que el valor especificado, se proporciona un NextToken en la salida del comando. Para reanudar la paginación, proporcione el valor de NextToken en el argumento `starting-token` de un comando posterior. No utilice el elemento de NextToken respuesta directamente fuera de la AWS CLI. Para ver ejemplos de uso, consulte [Paginación](#) en la Guía del usuario de la interfaz de línea de AWS comandos.

Tipo: entero

Rango válido: valor mínimo de 1. Valor máximo de 50.

Obligatorio: no

NextToken

Un token destinado a especificar dónde iniciar la paginación. Es el NextToken de una respuesta truncada anteriormente. Para ver ejemplos de uso, consulte [Paginación](#) en la Guía del usuario de la interfaz de línea de AWS comandos.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1000 caracteres.

Obligatorio: no

[RegionOptStatusContains](#)

Una lista de estados de región (habilitando, habilitada, deshabilitando, deshabilitada, habilitada por defecto) que se puede usar para filtrar la lista de regiones de una cuenta determinada. Por ejemplo, si se introduce un valor de HABILITANDO, solo se mostrará una lista de regiones con el estado de HABILITANDO.

Tipo: matriz de cadenas

Valores válidos: ENABLED | ENABLING | DISABLING | DISABLED |
ENABLED_BY_DEFAULT

Obligatorio: no

Sintaxis de la respuesta

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

{
  "NextToken": "string",
  "Regions": [
    {
      "RegionName": "string",
      "RegionOptStatus": "string"
    }
  ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[NextToken](#)

Si hay más datos que devolver, se rellenarán. Debe pasarse al parámetro de solicitud next-token de `list-regions`.

Tipo: cadena

[Regions](#)

Esta es una lista de regiones para una cuenta determinada o, si se utilizó el parámetro filtrado, una lista de regiones que coinciden con los criterios de filtro establecidos en el parámetro `filter`.

Tipo: matriz de objetos [Region](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AccessDeniedException

Se ha producido un error en la operación porque la identidad que ha realizado la llamada no tiene los permisos mínimos necesarios.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 403

InternalServerError

La operación falló debido a un error interno de AWS. Intente realizar la operación otra vez más tarde.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 500

TooManyRequestsException

Se ha producido un error en la operación porque se la ha llamado con demasiada frecuencia y ha superado la limitación.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 429

ValidationException

Se ha producido un error en la operación porque uno de los parámetros de entrada no era válido.

fieldList

El campo en el que se detectó la entrada no válida.

message

El mensaje donde se le informa qué no era válido en la solicitud.

reason

El motivo por el que se produjo un error en la validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET V4](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

PutAccountName

Actualiza el nombre de cuenta de la cuenta especificada. Para usar esta API, las entidades principales de IAM deben tener el permiso de `account:PutAccountName` IAM.

Sintaxis de la solicitud

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

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

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

AccountId

Especifica el número de ID de cuenta de 12 dígitos de la AWS cuenta a la que desea acceder o modificar con esta operación.

Si no especifica este parámetro, el valor predeterminado será la AWS cuenta de la identidad utilizada para llamar a la operación.

Para usar este parámetro, la persona que llama debe ser una identidad de la [cuenta de administración de la organización](#) o una cuenta de administrador delegado, y el ID de cuenta especificado debe ser una cuenta de miembro en la misma organización. La organización debe tener [todas las características habilitadas](#), así como el [acceso de confianza](#) habilitado para el servicio de administración de cuentas y, de manera opcional, puede tener asignada una cuenta de [administrador delegado](#).

Note

La cuenta de administración no puede especificar su propio AccountId; debe llamar a la operación en un contexto independiente al no incluir el parámetro AccountId.

Para llamar a esta operación en una cuenta que no es miembro de una organización, no especifique este parámetro y llame a la operación con una identidad que pertenezca a la cuenta cuyos contactos desea recuperar o modificar.

Tipo: cadena

Patrón: \d{12}

Obligatorio: no

AccountName

El nombre de la cuenta.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 50 caracteres.

Patrón: [- ; = ? - ~] +

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AccessDeniedException

Se ha producido un error en la operación porque la identidad que ha realizado la llamada no tiene los permisos mínimos necesarios.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 403

InternalServerErrorException

La operación falló debido a un error interno de AWS. Intente realizar la operación otra vez más tarde.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 500

TooManyRequestsException

Se ha producido un error en la operación porque se la ha llamado con demasiada frecuencia y ha superado la limitación.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 429

ValidationException

Se ha producido un error en la operación porque uno de los parámetros de entrada no era válido.

`fieldList`

El campo en el que se detectó la entrada no válida.

`message`

El mensaje donde se le informa qué no era válido en la solicitud.

`reason`

El motivo por el que se produjo un error en la validación.

Código de estado HTTP: 400

Ejemplos

Ejemplo 1

En el siguiente ejemplo, se actualiza el nombre para la cuenta cuyas credenciales se utilizan para llamar a la operación.

Solicitud de muestra

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

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

Respuesta de ejemplo

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

Ejemplo 2

En el siguiente ejemplo, se actualiza el nombre de cuenta para la cuenta de miembro especificada en una organización. Debe usar las credenciales de la cuenta de administración de la organización o de la cuenta de administrador delegado del servicio de Account Management.

Solicitud de muestra

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

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

Respuesta de ejemplo

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

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET V4](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

PutAlternateContact

Modifica el contacto alternativo especificado adjunto a un Cuenta de AWS.

Para obtener detalles sobre cómo utilizar las operaciones de contacto alternativo, consulte [Actualizar los contactos alternativos para su Cuenta de AWS](#).

Note

Antes de poder actualizar la información de contacto alternativa de una Cuenta de AWS empresa gestionada por AWS Organizations, primero debe habilitar la integración entre AWS Account Management y Organizations. Para obtener más información, consulte [Habilitación del acceso de confianza para la administración de la cuenta de AWS](#).

Sintaxis de la solicitud

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

{
  "AccountId": "string",
  "AlternateContactType": "string",
  "EmailAddress": "string",
  "Name": "string",
  "PhoneNumber": "string",
  "Title": "string"
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud


La solicitud acepta los siguientes datos en formato JSON.

AccountId

Especifica el número de ID de cuenta de 12 dígitos de la AWS cuenta a la que desea acceder o modificar con esta operación.

Si no especifica este parámetro, el valor predeterminado será la AWS cuenta de la identidad utilizada para llamar a la operación.

Para usar este parámetro, la persona que llama debe ser una identidad de la [cuenta de administración de la organización](#) o una cuenta de administrador delegado, y el ID de cuenta especificado debe ser una cuenta de miembro en la misma organización. La organización debe tener [todas las características habilitadas](#), así como el [acceso de confianza](#) habilitado para el servicio de administración de cuentas y, de manera opcional, puede tener asignada una cuenta de [administrador delegado](#).

 Note

La cuenta de administración no puede especificar su propio AccountId; debe llamar a la operación en un contexto independiente al no incluir el parámetro AccountId.

Para llamar a esta operación en una cuenta que no es miembro de una organización, no especifique este parámetro y llame a la operación con una identidad que pertenezca a la cuenta cuyos contactos desea recuperar o modificar.

Tipo: cadena

Patrón: `\d{12}`

Obligatorio: no

[AlternateContactType](#)

Especifica qué contacto alternativo desea crear o actualizar.

Tipo: cadena

Valores válidos: BILLING | OPERATIONS | SECURITY

Obligatorio: sí

[EmailAddress](#)

Especifica una dirección de correo electrónico para el contacto alternativo.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 254 caracteres.

Patrón: `[\s]*[\w+=.#|!&-]+@[\w.-]+\.[\w]+[\s]*`

Obligatorio: sí

Name

Especifica un nombre para el contacto alternativo.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 64.

Obligatorio: sí

PhoneNumber

Especifica un número de teléfono para el contacto alternativo.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 25 caracteres.

Patrón: `[\s0-9()+-]+`

Obligatorio: sí

Title

Especifica un título para el contacto alternativo.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 50 caracteres.

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AccessDeniedException

Se ha producido un error en la operación porque la identidad que ha realizado la llamada no tiene los permisos mínimos necesarios.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 403

InternalServerError

Se produjo un error en la operación debido a un error interno de AWS. Intente realizar la operación otra vez más tarde.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 500

TooManyRequestsException

Se ha producido un error en la operación porque se la ha llamado con demasiada frecuencia y ha superado la limitación.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 429

ValidationException

Se ha producido un error en la operación porque uno de los parámetros de entrada no era válido.

`fieldList`

El campo en el que se detectó la entrada no válida.

`message`

El mensaje donde se le informa qué no era válido en la solicitud.

reason

El motivo por el que se produjo un error en la validación.

Código de estado HTTP: 400

Ejemplos

Ejemplo 1

En el siguiente ejemplo, se establece el contacto alternativo de facturación para la cuenta cuyas credenciales se utilizan para llamar a la operación.

Solicitud de muestra

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

{
  "AlternateContactType": "Billing",
  "Name": "Carlos Salazar",
  "Title": "CFO",
  "EmailAddress": "carlos@example.com",
  "PhoneNumber": "206-555-0199"
}
```

Respuesta de ejemplo

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

Ejemplo 2

En el siguiente ejemplo, se establece o sobrescribe el contacto alternativo de facturación para la cuenta de miembro especificada en una organización. Debe usar las credenciales de la cuenta de administración de la organización o de la cuenta de administrador delegado del servicio de Account Management.

Solicitud de muestra

```
POST / HTTP/1.1
```

```
X-Amz-Target: AWSAccountV20210201.PutAlternateContact
```

```
{
  "AccountId": "123456789012",
  "AlternateContactType": "Billing",
  "Name": "Carlos Salazar",
  "Title": "CFO",
  "EmailAddress": "carlos@example.com",
  "PhoneNumber": "206-555-0199"
}
```

Respuesta de ejemplo

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

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET V4](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

PutContactInformation

Actualiza la información de contacto principal de una Cuenta de AWS.

Para obtener detalles sobre cómo utilizar las operaciones de contacto principal, consulte [Actualizar el contacto principal para su Cuenta de AWS](#).

Sintaxis de la solicitud

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

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

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.


Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

AccountId

Especifica el número de ID de cuenta de 12 dígitos al Cuenta de AWS que desea acceder o modificar con esta operación. Si no especifica este parámetro, el valor predeterminado será la

cuenta de Amazon Web Services de la identidad utilizada para llamar a la operación. Para usar este parámetro, la persona que llama debe ser una identidad de la [cuenta de administración de la organización](#) o una cuenta de administrador delegado. El ID de cuenta especificado debe ser una cuenta de miembro en la misma organización. La organización debe tener [todas las características habilitadas](#), así como el [acceso de confianza](#) habilitado para el servicio de administración de cuentas y, de manera opcional, puede tener asignada una cuenta de [administrador delegado](#).

 Note

La cuenta de administración no puede especificar su propio AccountId. Debe llamar a la operación en un contexto independiente al no incluir el parámetro AccountId.

Para llamar a esta operación en una cuenta que no es miembro de una organización, no especifique este parámetro. En su lugar, llame a la operación con una identidad que pertenezca a la cuenta cuyos contactos desea recuperar o modificar.

Tipo: cadena

Patrón: `\d{12}`

Obligatorio: no

[ContactInformation](#)

Contiene los detalles de la información de contacto principal asociada a una Cuenta de AWS.

Tipo: objeto [ContactInformation](#)

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AccessDeniedException

Se ha producido un error en la operación porque la identidad que ha realizado la llamada no tiene los permisos mínimos necesarios.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 403

InternalServerError

La operación falló debido a un error interno de AWS. Intente realizar la operación otra vez más tarde.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 500

TooManyRequestsException

Se ha producido un error en la operación porque se la ha llamado con demasiada frecuencia y ha superado la limitación.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 429

ValidationException

Se ha producido un error en la operación porque uno de los parámetros de entrada no era válido.

`fieldList`

El campo en el que se detectó la entrada no válida.

`message`

El mensaje donde se le informa qué no era válido en la solicitud.

reason

El motivo por el que se produjo un error en la validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET V4](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

StartPrimaryEmailUpdate

Inicia el proceso de actualización de la dirección de correo electrónico primaria de la cuenta especificada.

Sintaxis de la solicitud

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

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

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

AccountId

Especifica el número de ID de cuenta de 12 dígitos al Cuenta de AWS que desea acceder o modificar con esta operación. Para usar este parámetro, la persona que llama debe ser una identidad de la [cuenta de administración de la organización](#) o una cuenta de administrador delegado. El ID de cuenta especificado debe ser una cuenta de miembro en la misma organización. La organización debe tener [todas las características habilitadas](#), así como el [acceso de confianza](#) habilitado para el servicio de Account Management y, de manera opcional, puede tener asignada una cuenta de [administrador delegado](#).

Esta operación solo se puede realizar desde la cuenta de administración o desde la cuenta de administrador delegado de una organización para una cuenta de miembro.

Note

La cuenta de administración no puede especificar su propio AccountId.

Tipo: cadena

Patrón: \d{12}

Obligatorio: sí

[PrimaryEmail](#)

La nueva dirección de correo electrónico principal (también conocida como dirección de correo electrónico del usuario raíz) que se utilizará en la cuenta especificada.

Tipo: cadena

Restricciones de longitud: longitud mínima de 5 caracteres. La longitud máxima es de 64.

Obligatorio: sí

Sintaxis de la respuesta

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

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

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[Status](#)

El estado de la solicitud de actualización del correo electrónico principal.

Tipo: cadena

Valores válidos: PENDING | ACCEPTED

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

AccessDeniedException

Se ha producido un error en la operación porque la identidad que ha realizado la llamada no tiene los permisos mínimos necesarios.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 403

ConflictException

No se pudo procesar la solicitud debido a un conflicto en el estado actual del recurso. Esto ocurre, por ejemplo, si intenta activar una región que está deshabilitada actualmente (en estado EN PROCESO DE DESHABILITACIÓN) o si intenta cambiar el correo electrónico del usuario raíz de una cuenta por una dirección de correo electrónico que ya esté en uso.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 409

InternalServerError

La operación falló debido a un error interno de AWS. Intente realizar la operación otra vez más tarde.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 500

ResourceNotFoundException

Se ha producido un error en la operación porque se ha especificado un recurso que no se encuentra.

`errorType`

El valor que API Gateway rellena en el encabezado de respuesta de `x-amzn-ErrorType`.

Código de estado HTTP: 404

TooManyRequestsException

Se ha producido un error en la operación porque se la ha llamado con demasiada frecuencia y ha superado la limitación.

errorType

El valor que API Gateway rellena en el encabezado de respuesta de x-amzn-ErrorType.

Código de estado HTTP: 429

ValidationException

Se ha producido un error en la operación porque uno de los parámetros de entrada no era válido.

fieldList

El campo en el que se detectó la entrada no válida.

message

El mensaje donde se le informa qué no era válido en la solicitud.

reason

El motivo por el que se produjo un error en la validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS Interfaz de línea de comandos V2](#)
- [AWS SDK para .NET V4](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)

- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

Acciones relacionadas en otros AWS servicios

Las siguientes operaciones están relacionadas con el espacio de nombres de AWS Organizations, pero forman parte de él:

- [CreateAccount](#)
- [CreateGovCloudAccount](#)
- [DescribeAccount](#)

CreateAccount

La operación de `CreateAccount` API solo está disponible para su uso en el contexto de una organización gestionada por el AWS Organizations servicio. La operación de la API se define en el espacio de nombres de ese servicio.

Para obtener más información, consulta [CreateAccount](#) en la AWS Organizations Referencia de la API de .

CreateGovCloudAccount

La operación de `CreateGovCloudAccount` API solo está disponible para su uso en el contexto de una organización gestionada por el AWS Organizations servicio. La operación de la API se define en el espacio de nombres de ese servicio.

Para obtener más información, consulta [CreateGovCloudAccount](#) en la AWS Organizations Referencia de la API de .

DescribeAccount

La operación de `DescribeAccount` API solo está disponible para su uso en el contexto de una organización gestionada por el AWS Organizations servicio. La operación de la API se define en el espacio de nombres de ese servicio.

Para obtener más información, consulta [DescribeAccount](#) en la AWS Organizations Referencia de la API de .

Data Types

Los siguientes tipos de datos son compatibles:

- [AlternateContact](#)
- [ContactInformation](#)
- [Region](#)
- [ValidationExceptionField](#)

AlternateContact

Estructura que contiene los detalles de un contacto alternativo asociado a una cuenta de AWS

Contenido

AlternateContactType

El tipo de contacto alternativo.

Tipo: cadena

Valores válidos: BILLING | OPERATIONS | SECURITY

Obligatorio: no

EmailAddress

La dirección de correo electrónico asociada a este contacto alternativo.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 254 caracteres.

Patrón: `[\s]*[\w+=.#!&-]+@[\\w.-]+\\. [\w]+[\s]*`

Obligatorio: no

Name

El nombre asociado a este contacto alternativo.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 64.

Obligatorio: no

PhoneNumber

El número de teléfono asociado a este contacto alternativo.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 25 caracteres.

Patrón: `[\s0-9()+-]+`

Obligatorio: no

Title

El título asociado a este contacto alternativo.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 50 caracteres.

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ContactInformation

Contiene los detalles de la información de contacto principal asociada a una Cuenta de AWS.

Contenido

AddressLine1

La primera línea de la dirección de contacto principal.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 60 caracteres.

Obligatorio: sí

City

La ciudad de la dirección de contacto principal.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 50 caracteres.

Obligatorio: sí

CountryCode

El código ISO-3166 de dos letras de la dirección de contacto principal.

Tipo: cadena

Restricciones de longitud: longitud fija de 2 caracteres.

Obligatorio: sí

FullName

El nombre completo de la dirección de contacto principal.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 50 caracteres.

Obligatorio: sí

PhoneNumber

El número de teléfono de la información de contacto principal. El número se validará y, en algunos países, se comprobará para su activación.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 20 caracteres.

Patrón: `[+][\s0-9()-]+`

Obligatorio: sí

PostalCode

El código postal de la dirección de contacto principal.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 20 caracteres.

Obligatorio: sí

AddressLine2

La segunda línea de la dirección de contacto principal, si la hubiera.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 60 caracteres.

Obligatorio: no

AddressLine3

La tercera línea de la dirección de contacto principal, si la hubiera.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 60 caracteres.

Obligatorio: no

CompanyName

El nombre de la empresa asociada a la información de contacto principal, si la hubiera.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 50 caracteres.

Obligatorio: no

DistrictOrCounty

El distrito o condado de la dirección de contacto principal, si la hubiera.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 50 caracteres.

Obligatorio: no

StateOrRegion

El estado o la región de la dirección de contacto principal. Si la dirección postal se encuentra en los Estados Unidos (EE. UU.), el valor de este campo puede ser un código de estado de dos caracteres (por ejemplo, NJ) o el nombre completo del estado (por ejemplo, New Jersey). Este campo es obligatorio en los siguientes países: US, CA, GB, DE, JP, IN y BR.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 50 caracteres.

Obligatorio: no

WebsiteUrl

La URL del sitio web asociado a la información de contacto principal, si la hubiera.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

Region

Se trata de una estructura que expresa la región de una cuenta determinada y consta de un nombre y un estado de suscripción.

Contenido

RegionName

El código de región de una región determinada (por ejemplo, `us-east-1`).

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 50 caracteres.

Obligatorio: no

RegionOptStatus

Uno de los posibles estados que puede alcanzar una región (Habilitada, En proceso de habilitación, Deshabilitada, En proceso de deshabilitación, Habilitada por defecto).

Tipo: cadena

Valores válidos: `ENABLED` | `ENABLING` | `DISABLING` | `DISABLED` | `ENABLED_BY_DEFAULT`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ValidationExceptionField

La entrada no cumplía las restricciones especificadas por el AWS servicio en un campo específico.

Contenido

message

Un mensaje sobre la excepción de validación.

Tipo: cadena

Obligatorio: sí

name

El nombre del campo en el que se detectó la entrada no válida.

Tipo: cadena

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

Parámetros comunes

La siguiente lista contiene los parámetros que utilizan todas las acciones para firmar solicitudes de Signature Version 4 con una cadena de consulta. Los parámetros específicos de acción se enumeran en el tema correspondiente a la acción. Para obtener más información sobre la versión 4 de Signature, consulte [Firmar solicitudes de AWS API](#) en la Guía del usuario de IAM.

Action

Las acciones que se van a realizar.

Tipo: cadena

Obligatorio: sí

Version

La versión de API para la que está escrita la solicitud, expresada en el formato YYYY-MM-DD.

Tipo: cadena

Obligatorio: sí

X-Amz-Algorithm

El algoritmo de hash que utilizó para crear la solicitud de firma.

Condición: especifique este parámetro cuando incluya información de autenticación en una cadena de consulta en lugar de en el encabezado de autorización HTTP.

Tipo: cadena

Valores válidos: AWS4-HMAC-SHA256

Obligatorio: condicional

X-Amz-Credential

El valor del ámbito de la credencial, que es una cadena que incluye la clave de acceso, la fecha, la región a la que se dirige, el servicio que solicita y una cadena de terminación ("aws4_request"). El valor se expresa en el siguiente formato: access_key/AAAAMMDD/region/service/aws4_request.

Para obtener más información, consulte [Crear una solicitud de AWS API firmada](#) en la Guía del usuario de IAM.

Condición: especifique este parámetro cuando incluya información de autenticación en una cadena de consulta en lugar de en el encabezado de autorización HTTP.

Tipo: cadena

Obligatorio: condicional

X-Amz-Date

La fecha utilizada para crear la firma. El formato debe ser ISO 8601 formato básico (AAAAMMDD'T'HHMMSS'Z'). Por ejemplo, la siguiente fecha y hora es un X-Amz-Date valor válido:20120325T120000Z.

Condición: X-Amz-Date es opcional en todas las solicitudes; puede utilizarse para anular la fecha empleada para firmar solicitudes. Si el encabezado de fecha se especifica en el formato básico ISO 8601, no X-Amz-Date es obligatorio. Cuando X-Amz-Date se usa, siempre anula el valor del encabezado de fecha. Para obtener más información, consulte [Elementos de la firma de una solicitud de AWS API](#) en la Guía del usuario de IAM.

Tipo: cadena

Obligatorio: condicional

X-Amz-Security-Token

El token de seguridad temporal que se obtuvo mediante una llamada a AWS Security Token Service (AWS STS). Para obtener una lista de servicios compatibles con las credenciales de seguridad temporales de AWS STS, consulte [Servicios de AWS que funcionan con IAM](#) en la Guía del usuario de IAM.

Condición: si utilizas credenciales de seguridad temporales de AWS STS, debes incluir el token de seguridad.

Tipo: cadena

Obligatorio: condicional

X-Amz-Signature

Especifica la firma codificada hexadecimal que se calculó a partir de la cadena que se va a firmar y la clave de firma derivada.

Condición: especifique este parámetro cuando incluya información de autenticación en una cadena de consulta en lugar de en el encabezado de autorización HTTP.

Tipo: cadena

Obligatorio: condicional

X-Amz-SignedHeaders

Especifica todos los encabezados HTTP que se incluyeron como parte de la solicitud canónica. Para obtener más información sobre cómo especificar encabezados firmados, consulte [Crear una solicitud de AWS API firmada](#) en la Guía del usuario de IAM.

Condición: especifique este parámetro cuando incluya información de autenticación en una cadena de consulta en lugar de en el encabezado de autorización HTTP.

Tipo: cadena

Obligatorio: condicional

Errores comunes

En esta sección se enumeran los errores comunes a las acciones de la API de todos los AWS servicios. En el caso de los errores específicos de una acción de la API de este servicio, consulte el tema de dicha acción de la API.

AccessDeniedException

No tiene acceso suficiente para realizar esta acción.

Código de estado HTTP: 400

IncompleteSignature

La firma de la solicitud no se ajusta a AWS los estándares.

Código de estado HTTP: 400

InternalFailure

El procesamiento de la solicitud ha devuelto un error debido a un error o una excepción desconocidos.

Código de estado HTTP: 500

InvalidAction

La acción u operación solicitada no es válida. Compruebe que la acción se ha escrito correctamente.

Código de estado HTTP: 400

InvalidClientTokenId

El identificador de clave de AWS acceso o certificado X.509 proporcionado no existe en nuestros registros.

Código de estado HTTP: 403

NotAuthorized

No tiene permiso para realizar esta acción.

Código de estado HTTP: 400

OptInRequired

El identificador de clave de AWS acceso necesita una suscripción al servicio.

Código de estado HTTP: 403

RequestExpired

La solicitud llegó al servicio más de 15 minutos después del sello de fecha de la solicitud o más de 15 minutos después de la fecha de caducidad de la solicitud (por ejemplo, en el caso de los prefirados URLs), o el sello de fecha de la solicitud es más de 15 minutos en el futuro.

Código de estado HTTP: 400

ServiceUnavailable

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 503

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

Código de estado HTTP: 400

ValidationError

La entrada no cumple las restricciones especificadas por un AWS servicio.

Código de estado HTTP: 400

Llamar a la API mediante solicitudes de consulta HTTP

Esta sección contiene información general sobre el uso de la API de consultas para la administración de AWS cuentas. Para obtener más información acerca de las operaciones y los errores de la API, consulte la [referencia de la API](#).

Note

En lugar de realizar llamadas directas a la API de consultas de administración de AWS cuentas, puede utilizar una de las AWS SDKs. AWS SDKs Constan de bibliotecas y código

de muestra para varios lenguajes de programación y plataformas (Java, Ruby, .NET, iOS, Android y más). SDKs Proporcionan una forma cómoda de crear un acceso programático a la administración de AWS cuentas y AWS. Por ejemplo, se SDKs encargan de tareas como firmar criptográficamente las solicitudes, gestionar los errores y volver a intentar las solicitudes automáticamente. Para obtener información sobre AWS SDKs, incluido cómo descargarlos e instalarlos, consulte [Herramientas para Amazon Web Services](#).

Con la API de Query para la administración de AWS cuentas, puedes realizar acciones de servicio. Las solicitudes de la API de consulta son solicitudes HTTPS que deben contener un `Action` parámetro que indique la operación que se va a realizar. AWS La administración de cuentas admite GET y POST solicita todas las operaciones. Es decir, la API no requiere que use GET para algunas acciones y POST para otras. Sin embargo, las solicitudes GET están sujetas a las limitaciones de tamaño de una URL. Aunque este límite depende del navegador, suele ser de 2048 bytes. Por lo tanto, para las solicitudes de la API de consulta que requieran tamaños más grandes, debe utilizar una solicitud POST.

La respuesta es un documento XML. Para obtener más información acerca de la respuesta, consulte las páginas de cada acción en la [referencia de la API](#).

Temas

- [Puntos de conexión](#)
- [HTTPS obligatorio](#)
- [Firmar las solicitudes de AWS la API de administración de cuentas](#)

Puntos de conexión

AWS Account Management tiene un único punto final de API global que está alojado en el este de EE. UU. (Virginia del Norte) Región de AWS.

Para obtener más información sobre AWS los puntos de enlace y las regiones de todos los servicios, consulte [Regiones y puntos de enlace](#) en el. Referencia general de AWS

HTTPS obligatorio

Dado que la API de consulta puede devolver información confidencial como, por ejemplo, credenciales de seguridad, debe usar HTTPS para cifrar todas las solicitudes de la API.

Firmar las solicitudes de AWS la API de administración de cuentas

Las solicitudes deben firmarse con un ID de clave de acceso y una clave de acceso secreta. Te recomendamos encarecidamente que no utilices las credenciales de tu cuenta AWS raíz para el trabajo diario con la administración de AWS cuentas. Puedes usar las credenciales de un usuario AWS Identity and Access Management (de IAM) o credenciales temporales, como las que utilizas con un rol de IAM.

Para firmar tus solicitudes de API, debes usar la versión 4 de AWS Signature. Para obtener información sobre el uso de la versión 4 de Signature, consulte [Firmar las solicitudes de AWS API](#) en la Guía del usuario de IAM.

Para obtener más información, consulte los siguientes temas:

- [Credenciales de seguridad de AWS](#): ofrece información general acerca de los tipos de credenciales que puede utilizar para acceder a AWS.
- [Prácticas recomendadas de seguridad en IAM](#): ofrece sugerencias para usar el servicio de IAM para ayudar a proteger sus AWS recursos, incluidos los de la administración de AWS cuentas.
- [Credenciales temporales de seguridad en IAM](#): describe cómo crear y utilizar las credenciales temporales de seguridad.

Cuotas para AWS Account Management

Cuenta de AWS Tiene cuotas predeterminadas, anteriormente denominadas límites, para cada AWS servicio. A menos que se indique lo contrario, cada cuota es Región de AWS específica.

Cada una de ellas Cuenta de AWS tiene las siguientes cuotas relacionadas con la administración de cuentas.

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
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

Recurso	Cuota
Tasa de solicitudes <code>GetContactInformation</code> por cuenta	10 por segundo, ampliación a 15 por segundo
Tasa de solicitudes <code>GetGovCloudAccountInformation</code> por cuenta	3 por segundo, ampliación a 5 por segundo
Tasa de solicitudes <code>GetPrimaryEmail</code> por cuenta que llama	3 por segundo, ampliación a 3 por segundo
Tasa de solicitudes <code>GetRegionOptStatus</code> por cuenta	5 por segundo, ampliación a 5 por segundo
Tasa de solicitudes <code>ListRegions</code> por cuenta	5 por segundo, ampliación a 5 por segundo
Tasa de solicitudes <code>PutAccountName</code> por cuenta que llama	1 por segundo, ampliación a 1 por segundo
Tasa de solicitudes <code>PutAlternateContact</code> por cuenta	5 por segundo, ampliación a 8 por segundo
Tasa de solicitudes <code>PutContactInformation</code> por cuenta	5 por segundo, ampliación a 8 por segundo
Tasa de solicitudes <code>StartPrimaryEmailUpdate</code> por cuenta que llama	1 por segundo, ampliación a 1 por segundo

Administre las cuentas en India

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 descritos en 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 una Cuenta de AWS con AWS India](#)
- [Administre la información de verificación del cliente](#)

Crea una Cuenta de AWS con 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 abrir una cuenta AWS 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 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”](#).

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. Recibirá un correo electrónico de confirmación en cuanto se verifique el medio de pago y se active la cuenta.

 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 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 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 modifica los datos que utilizó anteriormente para la verificación del cliente, como el nombre o la dirección basada en la India que aparece en la información de contacto o facturación, es posible que tenga que actualizar y volver a enviar la información de verificación del 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.

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 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. 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.

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](#).
- Tarjeta de identificación de votante o EPIC: la tarjeta de identificación de votante, también conocida como tarjeta de identidad con fotografía (EPIC), contiene un número de identificación

único emitido por la Comisión Electoral de la India a los votantes elegibles de 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, tarjeta de votante o EPIC y pasaporte.
- Para cuentas comerciales: tarjeta PAN y certificado de constitución.

Administre su cuenta en AWS 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 [Configure su cuenta](#).

Utilice el Consola de administración de AWS 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”](#)
- [Edite varios números de impuestos sobre bienes y servicios \(GSTs\)](#)
- [Ver una factura fiscal](#)

Historial de documentos para la Guía del usuario de Account Management

En la siguiente tabla se describen las versiones de documentación de la administración de AWS cuentas.

Cambio	Descripción	Fecha
Nombre de cuenta nuevo APIs	Support para nuevos GetAccountInformation y PutAccountName APIs 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
Nuevo correo electrónico principal APIs	Support para nuevas GetPrimaryEmail y AcceptPrimaryEmailUpdate APIs para actualizar de forma centralizada la dirección de correo electrónico del usuario raíz StartPrimaryEmailUpdate , la dirección de para 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	6 de junio de 2024

	usuario de AWS Organizations	.
<u>Reescritura del tema de cierre de una cuenta</u>	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
<u>Fin de la compatibilidad para agregar nuevas preguntas de verificación de seguridad</u>	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
<u>Fin de la compatibilidad con el espacio de nombres aws-portal</u>	AWS Identity and Access Management (IAM) las acciones que anteriormente se utilizaban para administrar tu cuenta (por ejemplo, <code>aws-portal:ModifyAccount</code> y <code>yaws-portal:ViewAccount</code>) han llegado al final del soporte estándar.	1 de enero de 2024
<u>Reescritura del tema de las regiones</u>	Revisión completa de todo el tema de las regiones, incluida la adición de controles de expansión y contracción.	8 de octubre de 2023
<u>Reubicación de los temas para los usuarios raíz en la Guía del usuario de IAM</u>	Consolidación del debate sobre los usuarios raíz en un tema y enlaces de referencia 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 requisitos de número de teléfono y dirección de correo electrónico agregada.	12 de septiembre de 2023
Nueva información de contacto APIs	Support para nuevos GetContactInformation y PutContactInformation APIs.	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 versión original de inglés, prevalecerá la versión en inglés.