



Guía de referencia

# AWS Administración de cuentas



# AWS Administración de cuentas: Guía de referencia

Copyright © 2024 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

Bienvenido .....	1
¿Necesito varias Cuentas de AWS? .....	2
Administración de varias cuentas Cuentas de AWS .....	3
Primeros pasos: ¿Es la primera vez que lo usa AWS? .....	3
Requisitos previos .....	4
Paso 1: Crea tu Cuenta de AWS .....	5
Paso 2: Activa el MFA para tu usuario root .....	6
Paso 3: Cree un usuario administrador .....	7
Temas relacionados .....	7
Uso del usuario root .....	7
Administre su cuenta .....	9
Crear la cuenta de .....	9
Vea los identificadores de su cuenta .....	12
Encuentra tu Cuenta de AWS ID .....	13
Busque el seudónimo canónico de su Cuenta de AWS .....	15
Actualiza la configuración de tu cuenta .....	17
Entender los modos de funcionamiento de API .....	20
Concesión de permisos para actualizar atributos de cuentas .....	21
Actualiza la información de contacto de tu cuenta .....	23
Contactos de cuenta alternativos .....	24
Contacto de la cuenta principal .....	33
Actualice sus preguntas sobre los desafíos de seguridad .....	40
Especifica qué puede usar Regiones de AWS tu cuenta .....	42
Consideraciones antes de activar y desactivar las regiones .....	43
Habilita o deshabilita una región para cuentas independientes .....	46
Activa o desactiva una región de tu organización .....	48
Crea o actualiza el alias de tu cuenta .....	50
Facturación para su Cuenta de AWS .....	51
Administrar cuentas en India .....	51
Determina a qué empresa pertenece tu cuenta .....	52
Crea un Cuenta de AWS con AISPL .....	52
Administre su cuenta AISPL .....	54
Cierra tu cuenta .....	54
Lo que necesita saber antes de cerrar su cuenta .....	54

¿Cómo cerrar tu cuenta .....	56
¿Qué esperar después de cerrar la cuenta .....	59
Administración de cuentas y AWS Organizations .....	61
Acceso de confianza .....	62
Cuenta de administrador delegado .....	64
SCP de ejemplo .....	65
Seguridad .....	68
Protección de los datos .....	69
AWS PrivateLink .....	70
Creación del punto de enlace .....	70
Políticas de punto de enlace de Amazon VPC .....	71
Políticas de punto de enlace .....	71
Identity and Access Management .....	72
Público .....	73
Autenticación con identidades .....	73
Administración de acceso mediante políticas .....	77
AWSAdministración de cuentas e IAM .....	80
Ejemplos de políticas basadas en identidades .....	88
Uso de políticas basadas en identidades .....	92
Solución de problemas .....	94
Políticas administradas por AWS .....	97
AWSAccountManagementReadOnlyAccess .....	97
AWSAccountManagementFullAccess .....	98
Actualizaciones de políticas .....	99
Validación de conformidad .....	100
Resiliencia .....	101
Seguridad de infraestructuras .....	101
Supervisión .....	103
Registros de CloudTrail .....	103
Información de Administración de cuentas en CloudTrail .....	104
Descripción de las entradas de registro de administración de cuentas .....	105
Supervisar los eventos de administración de cuentas con EventBridge .....	108
Eventos de administración de cuentas .....	109
Referencia de la API .....	111
Acciones .....	113
DeleteAlternateContact .....	114

DisableRegion .....	119
EnableRegion .....	123
GetAlternateContact .....	127
GetContactInformation .....	133
GetRegionOptStatus .....	137
ListRegions .....	141
PutAlternateContact .....	146
PutContactInformation .....	152
Acciones relacionadas .....	155
CreateAccount .....	155
Crear una cuenta de Gov Cloud .....	155
DescribeAccount .....	155
Tipos de datos .....	156
AlternateContact .....	157
ContactInformation .....	159
Region .....	163
ValidationExceptionField .....	164
Parámetros comunes .....	164
Errores comunes .....	167
Realizar solicitudes de consulta HTTP .....	169
Puntos de conexión .....	170
HTTPS obligatorio .....	170
FirmandoAWSSolicitudes de API de administración de cuentas .....	170
Cuotas .....	171
Solución de problemas de su Cuenta de AWS .....	173
Problemas de creación de cuentas .....	173
No he recibido la llamada de AWS para verificar mi cuenta nueva .....	173
Cuando intento verificarlo mi Cuenta de AWS por teléfono, aparece un error sobre el "número máximo de intentos fallidos" .....	174
Han pasado más de 24 horas y mi cuenta no está activada .....	175
Problemas de cierre de cuentas .....	176
No sé cómo eliminar o cancelar mi cuenta .....	176
No veo el botón Cerrar cuenta en la página de cuentas .....	176
He cerrado mi cuenta pero aún no he recibido una confirmación por correo electrónico .....	176
Recibo un mensaje de error ConstraintViolationException «» al intentar cerrar mi cuenta ....	177

---

Recibo el mensaje de error «CLOSE_ACCOUNT_QUOTA_EXCEEDED» al intentar cerrar la cuenta de un miembro .....	177
¿Debo eliminar mi AWS organización antes de cerrar la cuenta de administración? .....	178
Otros problemas. ....	178
Quiero cambiar la tarjeta de crédito deCuenta de AWS .....	178
Quiero informar fraudulentaCuenta de AWSactividad .....	178
Quiero cerrar miCuenta de AWS .....	178
Historial de documentos .....	179
Glosario de AWS .....	181
.....	clxxxii

# Bienvenido a la Guía de referencia de administración de AWS cuentas

Cuentas de AWS son una parte fundamental del acceso a AWS los servicios.

Y Cuenta de AWS cumple dos funciones básicas:

- **Contenedor:** 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 (Amazon EC2) son todos recursos. Cada recurso se identifica de forma única mediante un nombre de recurso de Amazon (ARN) que incluye el ID de cuenta de la cuenta que contiene o 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 cree en su cuenta están disponibles para los usuarios que tengan 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 AWS). Las identidades también tienen políticas de permisos que especifican lo que un usuario puede hacer (autorización) con los recursos de la cuenta.

Como práctica recomendada de seguridad, exija a los usuarios que utilicen credenciales temporales al acceder AWS. Para proporcionar credenciales temporales, puede utilizar una [federación y un proveedor de identidad](#), como el [AWS IAM Identity Center](#) [IAM Identity Center](#). Si su empresa ya utiliza un proveedor de identidad, úselo con la federación para simplificar la forma en que proporciona acceso a los recursos de su Cuenta de AWS empresa.

Para obtener información sobre las prácticas recomendadas de seguridad, consulte las [prácticas recomendadas de seguridad en IAM](#) en la Guía del usuario de IAM.

## Temas

- [¿Necesito varias Cuentas de AWS?](#)
- [Primeros pasos: ¿Es la primera vez que lo usa AWS?](#)
- [Uso de la Usuario raíz de la cuenta de AWS](#)

## ¿Necesito varias Cuentas de AWS?

Cuentas de AWS sirven como límite de seguridad fundamental en AWS. Sirven como contenedor de recursos que proporciona un nivel útil de aislamiento. La capacidad de aislar recursos y usuarios es un requisito clave para establecer un entorno seguro y bien gobernado.

Separación de los recursos en separadas Cuentas de AWS le ayuda a admitir los siguientes principios en su entorno de nube:

- **Control de seguridad**— Las diferentes aplicaciones pueden tener distintos perfiles de seguridad, lo que requiere políticas y mecanismos de control diferentes a su alrededor. Por ejemplo, es mucho más fácil hablar con un auditor y poder apuntar a una sola Cuenta de AWS que aloja todos los elementos de la carga de trabajo que están sujetos a [Normas de seguridad para la industria de tarjetas de pago \(PCI\)](#).
- **Aislamiento**— Una Cuenta de AWS es una unidad de protección de seguridad. Los riesgos potenciales y las amenazas a la seguridad deben incluirse en una Cuenta de AWS sin afectar a otros. Puede haber diferentes necesidades de seguridad debido a diferentes equipos o perfiles de seguridad diferentes.
- **Muchos equipos**— Los diferentes equipos tienen sus diferentes responsabilidades y necesidades de recursos. Puedes evitar que los equipos interfieran entre sí moviéndolos a separadas Cuentas de AWS.
- **Aislamiento de datos**— Además de aislar a los equipos, es importante aislar los data stores en una cuenta. Esto puede ayudar a limitar el número de personas que pueden acceder y administrar ese data store. Esto ayuda a contener la exposición a datos altamente privados y, por lo tanto, puede ayudar en cumplimiento de [la Reglamentación 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 múltiples Cuentas de AWS, puede dar soporte a las necesidades específicas de una unidad de negocio.
- **Facturación**— Una cuenta es la única forma verdadera de separar los artículos a nivel de facturación. Varias cuentas ayudan a separar los artículos a nivel de facturación entre unidades de negocio, equipos funcionales o usuarios individuales. Aún puedes consolidar todas tus facturas en un único pagador (usando AWS Organizations y facturación consolidada) al tiempo que las líneas de pedido están separadas por Cuenta de AWS.



- Asignación de cuotas—AWSLas cuotas de servicio se aplican por separado para cada unoCuenta de AWS. Separación de cargas de trabajo en diferentesCuentas de AWSles impide consumir cuotas entre sí.

Todas las recomendaciones y procedimientos descritos en este documento se ajustan a la [AWSMarco de Well-Architected](#). Este marco está diseñado para ayudarlo a diseñar una infraestructura en la nube flexible, resistente y escalable. Incluso cuando empiezas a poco, te recomendamos que sigas cumpliendo esta guía en el marco. Hacerlo puede ayudarlo a escalar su entorno de forma segura y sin afectar sus operaciones en curso a medida que crece.

## Administración de varias cuentasCuentas de AWS

Antes de empezar a agregar varias cuentas, querrás desarrollar un plan para administrarlas. Para ello, le recomendamos que utilice [AWS Organizations](#), que es unAWSservicio para gestionar todos losCuentas de AWSen su organización.

AWS también ofrece AWS Control Tower, que añade capas deAWSautomatización administrada para Organizations y la integra automáticamente con otrosAWSservicios como AWS CloudTrail, AWS Config, Amazon CloudWatch, AWS Service Catalog, y otros. Estos servicios pueden generar costos adicionales. Para obtener más información, consulte [Precios de AWS Control Tower](#).

## Primeros pasos: ¿Es la primera vez que lo usaAWS?

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

### Pasos

- [Requisitos previos](#)
- [Paso 1: Crea tu Cuenta de AWS](#)
- [Paso 2: Activa el MFA para tu usuario root](#)
- [Paso 3: Cree un usuario administrador](#)
- [Temas relacionados](#)

## Requisitos previos

Para suscribirte a una Cuenta de AWS, necesitas la siguiente información:

- Un nombre de 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 pueda asignarles nombres que sean fáciles de reconocer. Para las cuentas de las empresas, considere la posibilidad de utilizar un estándar de nomenclatura, como organización, propósito, entorno (por ejemplo, AnyCompanyauditoría, producción). Para las cuentas personales, considere la posibilidad de utilizar un estándar de nomenclatura como nombre, apellidos y propósito (por ejemplo, paulo-santos-testaccount).

Para obtener información sobre cómo cambiar el nombre de una cuenta, consulta [¿Cómo cambio el nombre de mi cuenta Cuenta de AWS?](#) .

- Dirección: si tu dirección de contacto está en la India, el acuerdo de usuario de tu cuenta es con Amazon Internet Services Private Limited (AISPL), un AWS vendedor local de la India. Debe proporcionar su CVV como parte del proceso de verificación. Es posible que también tengas que introducir una contraseña de un solo uso, según tu banco. AISPL cobra 2 INR a tu método de pago como parte del proceso de verificación. AISPL reembolsará las 2 INR cuando haya concluido la verificación.
- Una dirección de correo electrónico: la dirección de correo electrónico se utiliza como nombre de inicio de sesión del usuario raíz y es necesaria para la recuperación de la cuenta. Debe poder recibir los mensajes de correo electrónico que se envíen a esta dirección. Antes de poder realizar determinadas tareas, debe comprobar que tiene acceso al correo electrónico enviado a esta dirección.

### 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 usar para restablecer las credenciales del usuario raíz de la cuenta, proteja el acceso a esta lista o dirección de distribución.

- Un número de teléfono: este número se puede usar para confirmar la propiedad de tu cuenta. Debes poder recibir llamadas a este número de teléfono.

### Important

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

## Paso 1: Crea tu Cuenta de AWS

1. En tu navegador, abre la [página de AWS inicio](#).
2. Selecciona Crear un Cuenta de AWS.


### Note

Si has iniciado sesión AWS recientemente, selecciona Iniciar sesión. Si la opción Crear una nueva Cuenta de AWS no está visible, primero selecciona Iniciar sesión en otra cuenta y, a continuación, selecciona Crear una nueva Cuenta de AWS.

3. Introduce la información de tu cuenta y, a continuación, selecciona Verificar dirección de correo electrónico. Esto enviará un código de verificación a la dirección de correo electrónico que especifiques.
4. Introduce tu código de verificación y, a continuación, selecciona Verificar.
5. Introduce una contraseña segura para el usuario root, confírmala y, a continuación, selecciona Continuar. AWS requiere que la contraseña cumpla las siguientes condiciones:
  - Debe tener un mínimo de 8 caracteres y un máximo de 128 caracteres.
  - Debe incluir un mínimo de tres de los siguientes tipos de caracteres: mayúsculas, minúsculas, números y ! @ # \$ % ^ & \* ( ) < > [ ] { } | \_ + = símbolos.
  - No debe ser idéntico a su Cuenta de AWS nombre o dirección de correo electrónico.
6. Elija Empresarial o Personal. La diferencia entre estas opciones es la información que le solicitamos. Ambos tipos de cuentas tienen las mismas características y funciones.
7. Introduce tu información empresarial o personal. Consulte las recomendaciones de la sección [Requisitos previos](#) sobre la dirección de correo electrónico y el número de teléfono.

8. Lee y acepta el [acuerdo con el AWS cliente](#). Asegúrese de leer y comprender los términos del Acuerdo con el AWS cliente.
9. Elija Continuar (Continuar). En ese momento, recibirás un mensaje de correo electrónico para confirmar Cuenta de AWS que estás listo para usarlo. Puedes iniciar sesión en tu nueva cuenta con la dirección de correo electrónico y la contraseña que proporcionaste al registrarte. Sin embargo, no podrás usar ningún AWS servicio hasta que hayas terminado de activar tu cuenta.
10. Introduce la información sobre tu método de pago. Si quieres usar una dirección diferente para la facturación, selecciona Usar una dirección nueva.
11. Elija Verificar y continuar.
12. Introduce el código de tu país o región de la lista y, a continuación, introduce un número de teléfono con el que podamos contactar contigo en los próximos minutos. Introduce el código CAPTCHA y envíalo.
13. Cuando el sistema automatizado se ponga en contacto con usted, introduzca el PIN que reciba y, a continuación, envíelo.
14. Selecciona tu AWS Support plan. Para obtener una descripción de los planes disponibles, consulta [Comparar AWS Support planes](#).
15. Selecciona Completar registro. Aparece una página de confirmación que indica que tu cuenta se está activando.
16. Busca en tu carpeta de correo electrónico y correo no deseado un mensaje de correo electrónico que confirme que tu cuenta se ha activado. La activación suele tardar unos minutos, pero a veces puede tardar hasta 24 horas.

Tras recibir el mensaje de activación, tendrá acceso completo a todos los AWS servicios.

 Note

Si tiene problemas con la activación de la cuenta, consulte [the section called “Problemas de creación de cuentas”](#).

## Paso 2: Activa el MFA para tu usuario root

Le recomendamos encarecidamente que active el MFA para el usuario root. La MFA reduce drásticamente el riesgo de que alguien acceda a su cuenta sin su autorización.

1. Inicie sesión en [AWS Management Console](#) como propietario de cuenta eligiendo Usuario raíz e ingrese el email de su Cuenta de AWS. En la siguiente página, escriba su contraseña.

Para obtener ayuda para iniciar sesión con su usuario root, consulte [Iniciar sesión AWS Management Console como usuario root en la Guía del usuario](#) de AWS Inicio de sesión.

2. Activa el MFA para el usuario root.

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

## Paso 3: Cree un usuario administrador

Como no puede restringir lo que puede hacer un usuario root, le recomendamos encarecidamente que no lo utilice para tareas que no requieran explícitamente al usuario root. En su lugar, asigne el acceso administrativo a un usuario administrativo en el Centro de identidades de IAM e inicie sesión como ese usuario administrativo para realizar sus tareas administrativas diarias.

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

## Temas relacionados

- Para obtener información sobre cómo proteger las credenciales del usuario raíz, consulte [Cómo proteger las credenciales del usuario raíz en la Guía del usuario](#) de IAM.
- Para ver una lista de las tareas que requieren el usuario raíz, consulte [las tareas que requieren credenciales de usuario raíz](#) en la Guía del usuario de IAM.

## Uso de la Usuario raíz de la cuenta de AWS

### Important

Cualquier persona que tenga credenciales de usuario raíz para su Cuenta de AWS dispondrá de acceso ilimitado a todos los recursos de su cuenta, incluida la información de facturación.

Cuando se crea una Cuenta de AWS, se comienza con una identidad de inicio de sesión que tiene acceso completo a todos los recursos y Servicios de AWS de la cuenta. Esta identidad recibe el

nombre de usuario raíz de la Cuenta de AWS y se accede a ella iniciando sesión con el email y la contraseña que utilizó para crear la cuenta. Recomendamos que no utilice el usuario raíz para las tareas cotidianas. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que este pueda realizar. Para obtener 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.

Para evitar utilizar el usuario root en las tareas diarias, aprenda a [configurar un usuario administrativo en AWS IAM Identity Center](#). Para obtener más recomendaciones de seguridad para los [usuarios root](#), consulte [las mejores prácticas para los usuarios root](#) Cuenta de AWS.

Puede [cambiar](#) o [restablecer la contraseña del usuario raíz](#) y [crear](#) o [eliminar claves de acceso \(ID de clave de acceso y claves de acceso secretas\)](#) para su usuario raíz. Si necesitas ayuda para iniciar sesión con tu usuario root, consulta [Iniciar sesión AWS Management Console como usuario root en la Guía del usuario](#) de AWS inicio de sesión.

# Administre su Cuenta de AWS

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

## Note

Si tu Cuenta de AWS se creó en la India utilizando Amazon Internet Services Private Limited (AISPL), hay consideraciones adicionales. Para obtener más información, consulte [Administrar cuentas en India](#).

## Temas

- [Crea una versión independiente Cuenta de AWS](#)
- [Ver Cuenta de AWS identificadores](#)
- [Actualice el Cuenta de AWS nombre, la dirección de correo electrónico o la contraseña del usuario root](#)
- [Entender los modos de funcionamiento de API](#)
- [Actualice su Cuenta de AWS información de contacto](#)
- [Actualizar las preguntas sobre desafíos de seguridad](#)
- [Especifica qué puede usar Regiones de AWS tu cuenta](#)
- [Crea o actualiza tu Cuenta de AWS alias](#)
- [Facturación para su Cuenta de AWS](#)
- [Administrar cuentas en India](#)
- [Cerrar un Cuenta de AWS](#)

## Crea una versión independiente Cuenta de AWS

En este tema se describe cómo crear una versión independiente Cuenta de AWS que no esté gestionada por AWS Organizations. Si desea crear una cuenta que forme parte de una organización administrada por AWS Organizations, consulte [Crear una cuenta de miembro en su organización en la Guía del AWS Organizations usuario](#).

Estas instrucciones son para crear una empresa Cuenta de AWS fuera de la India. Para crear una cuenta en la India, consulte [Crea un Cuenta de AWS con AISPL](#).

## AWS Management Console

Para crear un Cuenta de AWS

1. Abre la [página de inicio de Amazon Web Services](#).
2. Elija Crear un Cuenta de AWS.

### Note

Si has iniciado sesión AWS recientemente, es posible que esa opción no esté disponible. En su lugar, selecciona Iniciar sesión en la consola. A continuación, si Crear una nueva Cuenta de AWS aún no está visible, selecciona Iniciar sesión en otra cuenta y, a continuación, selecciona Crear una nueva Cuenta de AWS.

3. Introduce la información de tu cuenta y, a continuación, selecciona Verificar dirección de correo electrónico. Esto enviará un código de verificación a la dirección de correo electrónico que especifiques.

### Important


Debido a la naturaleza crítica del [usuario root](#) de la cuenta, te recomendamos encarecidamente que utilices una dirección de correo electrónico a la que pueda acceder un grupo y no solo una persona. De esta forma, si la persona que se registró Cuenta de AWS deja la empresa, Cuenta de AWS podrá seguir utilizándola, ya que la dirección de correo electrónico seguirá siendo accesible.

Si pierdes el acceso a la dirección de correo electrónico asociada a la cuenta Cuenta de AWS, no podrás recuperar el acceso a la cuenta si alguna vez pierdes la contraseña.

4. Introduce tu código de verificación y, a continuación, selecciona Verificar.
5. Introduce una contraseña segura para el usuario root, confírmala y, a continuación, selecciona Continuar. AWS requiere que la contraseña cumpla las siguientes condiciones:
  - Debe tener 8 caracteres como mínimo y 128 como máximo.
  - Debe incluir, como mínimo, tres de estos tipos de caracteres combinados: mayúsculas, minúsculas, números y símbolos ! @ # \$ % ^ & \* ( ) < > [ ] { } | \_ +=.
  - No debe ser idéntica al nombre de la Cuenta de AWS ni a la dirección de correo electrónico.



6. Elija Empresarial o Personal. Las cuentas personales y las cuentas empresariales tienen las mismas características y funciones.
7. Introduzca su información empresarial o 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.
- Una dirección de correo electrónico con un nombre de dominio que pertenezca a la empresa u organización que utilizará la cuenta.

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.

8. Lee y acepta el [Acuerdo de AWS cliente](#). Asegúrese de leer y comprender los términos del Acuerdo con el AWS cliente.
9. Elija Continue (Continuar). En ese momento, recibirás un mensaje de correo electrónico para confirmar Cuenta de AWS que estás listo para usarlo. Puedes iniciar sesión en tu nueva cuenta con la dirección de correo electrónico y la contraseña que proporcionaste al registrarte. Sin embargo, no podrás usar ningún AWS servicio hasta que hayas terminado de activar tu cuenta.
10. Introduce la información sobre tu método de pago y, a continuación, selecciona Verificar y continuar. Si quieres usar una dirección de facturación diferente para tu información AWS de facturación, selecciona Usar una dirección nueva.

No puedes continuar con el proceso de registro hasta que agregues un método de pago válido.

11. Introduce el código de tu país o región de la lista y, a continuación, introduce un número de teléfono con el que podamos contactar contigo en los próximos minutos.
12. Introduce el código que aparece en el CAPTCHA y, a continuación, envíalo.
13. Cuando el sistema automatizado se ponga en contacto con usted, introduzca el PIN que reciba y, a continuación, envíelo.
14. Selecciona uno de los AWS Support planes disponibles. Para obtener una descripción de los planes Support disponibles y sus beneficios, consulte [Comparar AWS Support planes](#).

15. Elija Completar registro. Aparece una página de confirmación que indica que tu cuenta se está activando.
16. Busca en tu carpeta de correo electrónico y correo no deseado un mensaje de correo electrónico que confirme que tu cuenta se ha activado. La activación suele tardar unos minutos, pero a veces puede tardar hasta 24 horas.

Tras recibir el mensaje de activación, tendrá acceso completo a todos los AWS servicios.

## 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.

## 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, como 012345678901, que identifica de forma exclusiva a un. Cuenta de AWS Muchos AWS recursos incluyen el ID de la cuenta en sus [nombres de recursos de Amazon \(ARN\)](#). La parte del ID de cuenta distingue los recursos de una cuenta de los recursos de otra cuenta. Si eres usuario AWS Identity and Access Management (de IAM), puedes iniciar sesión en ella AWS Management Console con el ID o el alias de la cuenta. Si bien los ID de cuenta, al igual que cualquier información de identificación, deben usarse y compartirse con cuidado, no se consideran información secreta, sensible o confidencial.

### [ID de usuario canónico](#)

Un identificador alfanumérico, por ejemplo 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be, una forma ofuscada del ID. 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 su seudónimo canónico como usuario [raíz o Cuenta de AWS como usuario](#) de IAM.

Debe estar autenticado para ver estos identificadores AWS .

### 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 () AWS Management Console o las teclas AWS Command Line Interface (AWS CLI). En la consola, la ubicación del ID de la cuenta depende de si has iniciado sesión como usuario root o como usuario de IAM. El ID de cuenta es el mismo tanto si has iniciado sesión como usuario root como si eres usuario de IAM.

### Buscar el ID de tu cuenta como usuario raíz

#### AWS Management Console

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 inicias sesión como usuario root, no necesitas ningún permiso de IAM.

1. En la barra de navegación de la esquina superior derecha, elige el nombre o número de tu cuenta y, a continuación, selecciona Credenciales de seguridad.

#### Tip

Si no ves la opción Credenciales de seguridad, es posible que hayas iniciado sesión como usuario federado con un rol de IAM, en lugar de como usuario de IAM. En este caso, busca 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 Cuenta de AWS ID.

## 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 root, no necesita ningún permiso de IAM.

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

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

## Busca tu ID de cuenta como usuario de IAM

### AWS Management Console

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 su nombre de usuario y, a continuación, elija Credenciales de seguridad.

### Tip

Si no ves la opción Credenciales de seguridad, es posible que hayas iniciado sesión como usuario federado con un rol de IAM, en lugar de como usuario de IAM. En este caso, busca 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 a la Cuenta de AWS ID.

## AWS CLI & SDKs

Para encontrar tu Cuenta de AWS ID usando el AWS CLI

### Permisos mínimos

Para realizar los siguientes pasos, debe tener al menos los siguientes permisos IAM:

- Al ejecutar el comando como usuario o rol 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
```

## Busque el seudónimo canónico de su Cuenta de AWS

Puede encontrar su seudónimo canónico Cuenta de AWS utilizando el o el. AWS Management Console AWS CLIEl 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.

## Busque el ID canónico como usuario raíz o usuario de IAM

### AWS Management Console


Para encontrar el seudónimo canónico de tu cuenta al iniciar sesión en la consola como usuario root o usuario de IAM

### Permisos mínimos

Para realizar los siguientes pasos, debe tener al menos los siguientes permisos IAM:

- Cuando ejecutas el comando como usuario root, no necesitas ningún permiso de IAM.
- Al iniciar sesión como usuario de IAM, debe tener:
  - `account:GetAccountInformation`

1. Inicie sesión AWS Management Console como usuario root o usuario de IAM.
2. En la barra de navegación de la parte superior derecha, elige el nombre o número de tu cuenta y, a continuación, selecciona Credenciales de seguridad.

 Tip

Si no ves la opción Credenciales de seguridad, es posible que hayas iniciado sesión como usuario federado con un rol de IAM, en lugar de como usuario de IAM. En este caso, busca la entrada Cuenta y el número de ID de cuenta que aparece junto a ella.

3. En la sección Detalles de la cuenta, el seudónimo canónico aparece junto al seudónimo canónico. Puede usar su seudónimo canónico para configurar las listas de control de acceso (ACL) de Amazon S3.

## AWS CLI & SDKs

Para encontrar el ID de usuario canónico mediante el AWS CLI

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

Utilice el comando [list-buckets](#) de la siguiente manera.

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

## Busque el ID canónico como usuario federado con una función de IAM

### AWS Management Console

Para encontrar el ID canónico de tu cuenta al iniciar sesión en la consola como usuario federado con un rol de IAM

#### Permisos mínimos

- Debe tener permiso para publicar y ver un bucket de Amazon S3.

1. Inicie sesión AWS Management Console 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 de la lista de control de acceso, en Propietario del bucket, aparece tu Cuenta de AWS ID canónico.

### AWS CLI & SDKs

Para encontrar el seudónimo canónico, usa el AWS CLI

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


Utilice el comando [list-buckets](#) de la siguiente manera.

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

## Actualice el Cuenta de AWS nombre, la dirección de correo electrónico o la contraseña del usuario root

Para editar su Cuenta de AWS nombre o cambiar la contraseña o la dirección de correo electrónico del usuario root, lleve a cabo los pasos del siguiente procedimiento. Esta dirección de correo


electrónico y la contraseña son las credenciales que utiliza para iniciar sesión como Usuario raíz de la cuenta de AWS.

 Note

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

## AWS Management Console


Para editar su Cuenta de AWS nombre, contraseña o dirección de correo electrónico del usuario raíz

 Permisos mínimos

Para realizar los siguientes pasos, debe tener al menos los siguientes permisos IAM:

- 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 [AWS Management Console](#) 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 Configuración de la cuenta, elija Editar. Se le solicitará que vuelva a autenticarse por motivos de seguridad.


 Note

Si no ve la opción Editar, es probable que no haya iniciado sesión como el usuario raíz de la cuenta. No puede modificar la configuración de la cuenta si ha iniciado sesión como usuario o rol de IAM.

4. En la página Actualizar la configuración de la cuenta, selecciona Editar junto al campo que deseas actualizar.




- a. Para el nombre: en la página Actualizar el nombre de la cuenta, en Nombre de cuenta nuevo, introduce el nombre de la nueva cuenta y, a continuación, selecciona Guardar cambios.

 Note

Si no puede modificar el Cuenta de AWS nombre, compruebe si existe una política de control de servicios (SCP) AWS Organizations que restrinja el acceso `account` o deniegue la `iam:UpdateAccountName` acción.

- b. Para el correo electrónico: en la página Actualiza tu dirección de correo electrónico, rellena los campos Nueva dirección de correo electrónico, Confirma la nueva dirección de correo electrónico y confirma tu contraseña actual. A continuación, elija Save changes (Guardar cambios). Se envía un código de verificación a tu nueva dirección de correo electrónico desde `no-reply@verify.signin.aws`. En la página Verifica tu nueva dirección de correo electrónico, en Código de verificación, introduce el código que recibiste de tu correo electrónico y, a continuación, selecciona Guardar cambios.

 Note

El código de verificación puede tardar hasta 5 minutos en llegar. Si no ves el correo electrónico en tu bandeja de entrada, revisa tus carpetas de spam y correo basura.

- c. Para la contraseña: en la página Actualizar la contraseña, rellena los campos Contraseña actual, Contraseña nueva y Confirma la nueva contraseña. A continuación, elija Save changes (Guardar cambios). Para obtener más información, incluidas las mejores prácticas para configurar las contraseñas de los usuarios raíz, consulte [Cambiar la contraseña de Usuario raíz de la cuenta de AWS](#) la Guía del usuario de IAM.
5. Después de realizar todos los cambios, elija Done (Hecho).

## AWS CLI & SDKs

Esta tarea no es compatible con la AWS CLI o con una operación de API de uno de los AWS SDK. Solamente puede realizar esta tarea mediante la AWS Management Console.

# Entender los modos de funcionamiento de API

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

- **Contexto independiente**— este modo se utiliza cuando un usuario o rol de una cuenta accede o cambia un atributo de cuenta en la misma cuenta. El modo de contexto independiente se utiliza automáticamente cuando no se incluye `AccountId` al llamar a uno de los parámetros de Administración de cuentas AWS CLI o AWS Operaciones de SDK.
- **Contexto de Organizations**— este modo se utiliza cuando un usuario o rol de una cuenta de una organización accede o cambia un atributo de cuenta en una cuenta de miembro diferente de la misma organización. El modo de contexto de la organización se usa automáticamente cuando se incluye `AccountId` al llamar a uno de los parámetros de Administración de cuentas AWS CLI o AWS Funcionamiento del SDK. Puede llamar a las operaciones en este modo solo desde la cuenta de administración de la organización o la cuenta de administrador delegada para Administración de cuentas.

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

- Si no se incluye `AccountId`, la operación se ejecuta en el contexto independiente y aplica automáticamente la solicitud a la cuenta que utilizó para realizar la solicitud. Esto es cierto independientemente de que la cuenta sea miembro de una organización o no.
- Si incluye el `AccountId`, la operación se ejecuta en el contexto de la organización y la operación funciona en la cuenta Organizations especificada.
  - Si la cuenta que llama a la operación es la cuenta de administración o la cuenta de administrador delegado para el servicio de administración de cuentas, puede especificar cualquier cuenta de miembro de esa organización en `AccountId` para actualizar la cuenta de 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 `AccountId` es la cuenta especificada como [Cuenta de administrador delegado](#) para el servicio de gestión de cuentas. Cualquier otra cuenta, incluida la cuenta de administración, recibe un `AccessDenied` excepción.
- Si ejecuta una operación en modo independiente, debe tener permiso para ejecutar la operación con una política de IAM que incluya un `Resource` elemento de cualquiera "\*" para permitir todos los recursos, o [ARN que usa la sintaxis de una cuenta independiente](#).

- Si ejecuta una operación en modo de organización, debe tener permiso para ejecutar la operación con una política de IAM que incluya `Resource` de cualquiera "\*" para permitir todos los recursos, o [ARN que usa la sintaxis de una cuenta de miembro en una organización](#).

## Concesión de permisos para actualizar atributos de cuentas

Como ocurre con la mayoría de operaciones de AWS, se conceden permisos para añadir, actualizar o eliminar atributos de cuenta para Cuentas de AWS al usar [Políticas de permisos de IAM](#). Al adjuntar una política de permisos de IAM a una entidad principal de IAM (un usuario o rol), debe especificar qué acciones puede realizar esa entidad principal sobre qué recursos y en qué condiciones.

Las siguientes son algunas consideraciones específicas de la administración de cuentas para crear una política de permisos.

### Formato de Nombre de recurso de Amazon para Cuentas de AWS

- [El nombre de recurso de Amazon \(ARN\)](#) para una Cuenta de AWS que puedes incluir en la `Resource` 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 sobre [Entender los modos de funcionamiento de API](#).

- Un ARN de cuenta para una cuenta independiente:

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

Debe usar este formato cuando ejecute una operación de atributos de cuenta en modo independiente sin incluir el `AccountID` parámetro.

- Un ARN de cuenta para una cuenta miembro de una organización:

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

Debe usar este formato cuando ejecute una operación de atributos de cuenta en modo de organizaciones mediante la inclusión de `AccountID` parámetro.

## Claves de contexto para políticas IAM

El servicio de administración de cuentas también ofrece varios [Claves de condición específicas del servicio de Administración de cuentas](#) que proporcionan un control detallado sobre los permisos que usted concede.

### **account:AccountResourceOrgPaths**

La clave de contexto `account:AccountResourceOrgPaths` permite especificar una ruta a través de la jerarquía de su organización hasta una unidad organizativa (OU) específica. Solo las cuentas de miembros que contiene esa unidad organizativa coinciden con la condición. El siguiente fragmento de ejemplo restringe la política para que se aplique solo a las cuentas que se encuentran en cualquiera de las dos unidades organizativas especificadas.

Porque `account:AccountResourceOrgPaths` es un tipo de cadena con varios valores, debe usar [la `ForAnyValue` o `ForAllValues` operadores de cadenas de valores múltiples](#). Además, tenga en cuenta que el prefijo de la clave de condición es `account`, aunque esté haciendo referencia a las rutas a las unidades organizativas de una organización.

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

### **account:AccountResourceOrgTags**

La clave de contexto `account:AccountResourceOrgTags` permite hacer referencia a las etiquetas que se pueden adjuntar a una cuenta de una organización. Una etiqueta es un par de cadenas clave/valor que puedes usar para clasificar y etiquetar los recursos de tu cuenta. Para obtener más información sobre el etiquetado, consulte [Editor de etiquetas de](#) en la [AWS Resource Groups Guía del usuario](#). Para obtener información sobre el uso de etiquetas como parte de una estrategia de control de acceso basado en atributos, consulte [Qué es ABAC para AWS](#) en la [IAM User Guide](#). El siguiente fragmento de ejemplo restringe la política para que se aplique solo a las cuentas de una organización que tengan la etiqueta con la clave `projecty` un valor de `blueoored`.

Porque `account:AccountResourceOrgTags` es un tipo de cadena con varios valores, debe usar [la `ForAnyValueForAllValues` operadores de cadenas de valores múltiples](#). Además, tenga en cuenta que el prefijo de la clave de condición es `account`, aunque haga referencia a las etiquetas de la cuenta de miembro de una organización.

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

#### Note

Puedes adjuntar etiquetas solo a una cuenta de una organización. No puede adjuntar etiquetas a un dispositivo independiente Cuenta de AWS.

## Actualice su Cuenta de AWS información de contacto

Puede almacenar información de contacto sobre el [contacto principal de la cuenta](#) para tu Cuenta de AWS. También puede añadir o editar la información de contacto para lo siguiente: [contactos de cuenta alternativos](#):

- **Facturación**— El contacto de facturación alternativo recibirá notificaciones relacionadas con la facturación, como las notificaciones de disponibilidad de facturas.
- **Operaciones**— El contacto de operaciones alternativo recibirá notificaciones relacionadas con las operaciones.
- **Seguridad**— El contacto de seguridad alternativo recibirá notificaciones relacionadas con la seguridad, incluidas las notificaciones del AWS Equipo de abuso.

### Temas

- [Actualiza los contactos alternativos para tu Cuenta de AWS](#)
- [Actualiza el contacto principal de tu Cuenta de AWS](#)

## Actualiza los contactos alternativos para tu Cuenta de AWS

Los contactos alternativos AWS permiten contactar con hasta tres contactos alternativos asociados a la cuenta. Un contacto alternativo no tiene por qué 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.

Puedes especificar solo uno de los siguientes tipos de contacto asociados a una cuenta.

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

Puedes añadir 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 y SDK. Para obtener información sobre cómo hacerlo, consulte [Actualizar contactos alternativos independientes. Cuenta de AWS](#)
- **Cuentas de AWS dentro de una organización:** en el caso de las cuentas de miembros que forman parte de una AWS organización, un usuario de la cuenta de administración o de la cuenta de administrador delegado puede actualizar de forma centralizada cualquier cuenta de miembro de la organización desde la AWS Organizations consola o mediante programación mediante la AWS CLI y los SDK. Para obtener información sobre cómo hacerlo, consulta [Actualizar contactos Cuenta de AWS alternativos](#) en tu organización.

### Temas

- [Requisitos de número de teléfono y dirección de correo electrónico](#)
- [Actualice los contactos alternativos para convertirlos en contactos independientes Cuenta de AWS](#)
- [Actualice los contactos alternativos de cualquier Cuenta de AWS parte 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 tu cuenta, te recomendamos que revises primero los siguientes requisitos al introducir 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 y pueden 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 convertirlos en contactos independientes 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 AWS Management Console procedimiento siguiente siempre funciona solo en el contexto independiente. Puede utilizar el AWS Management Console para acceder o cambiar únicamente los contactos alternativos de la cuenta que utilizó para llamar a la operación.

### AWS Management Console


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 [AWS Management Console](#) como usuario o rol de IAM que tenga los permisos mínimos.
2. Elige el nombre de tu cuenta en la parte superior derecha de la ventana y, a continuación, selecciona Cuenta.
3. En la página de la cuenta, desplázate hacia abajo hasta Contactos alternativos y, a la derecha del título, selecciona Editar.

 Note

Si no ves la opción Editar, es probable que no hayas iniciado sesión como usuario root de tu cuenta o como alguien que tenga los permisos mínimos especificados anteriormente.

4. Cambie los valores de cualquiera de los campos disponibles.

 Important

En el caso de las empresas Cuentas de AWS, se recomienda introducir el número de teléfono y la dirección de correo electrónico de la empresa en lugar de los de una persona física.

5. Una vez que haya realizado todos los cambios, elija Actualizar.

## 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 con las cuentas de los miembros, debes [habilitar el acceso confiable al servicio de cuentas](#).

### Permisos mínimos

Para cada operación, debes tener el permiso correspondiente 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 utilizas estos permisos individuales, puedes 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 Operations 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 realiza 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 intentas eliminar el mismo contacto más de una vez, el primero lo hará de forma silenciosa. Todos los intentos posteriores generan una ResourceNotFound excepción.

## Actualice los contactos alternativos de cualquier Cuenta de AWS parte de su organización

Para añadir 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 funciones para administrar la configuración de las cuentas de sus miembros. Esto permite al administrador controlar las cuentas de los miembros. Esto se establece de forma predeterminada al crear la organización. Si su organización está configurada únicamente para la facturación unificada y desea habilitar todas las funciones, consulte [Habilitar todas las funciones en su organización](#).
- Debe habilitar el acceso confiable al servicio de administración de AWS cuentas. Para configurarlo, consulte [Habilitar 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 las API de administración de AWS cuentas, de forma que puedas acceder a los datos de las cuentas desde la AWS Organizations consola. Para ver las políticas administradas actualizadas, consulte [Actualizaciones de las políticas AWS administradas por Organizations](#).

### AWS Management Console

Para agregar o editar los contactos alternativos de cualquier parte Cuenta de AWS de su organización

1. Inicie sesión en la [AWS Organizations consola](#) con las credenciales de la cuenta de administración de la organización.
2. Desde Cuentas de AWS, selecciona la cuenta que deseas actualizar.

3. Selecciona Información de contacto y, en Contactos alternativos, busca el tipo de contacto: contacto de facturación, contacto de seguridad o contacto de operaciones.
4. Para agregar un contacto nuevo, selecciona Agregar, o para actualizar un contacto existente, selecciona 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. Una vez que haya realizado todos los cambios, elija Actualizar.


## 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 con las cuentas de los miembros, debes [habilitar el acceso confiable al servicio de cuentas](#).
- No puedes acceder a una cuenta de una organización diferente a la que utilizas para llamar a la operación.

 Permisos mínimos

Para cada operación, debes tener el permiso correspondiente 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 utilizas estos permisos individuales, puedes 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 la administración de cuentas.

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

### Example

En el siguiente ejemplo, se establece el contacto alternativo de Operaciones para la cuenta de miembro especificada en una organización. Las credenciales utilizadas deben provenir de la cuenta de administración de la organización o de la cuenta de administrador delegado de la administración de cuentas.

```
$ 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, el primero 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 la administración de cuentas.

```
$ 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 intentas eliminar el mismo contacto más de una vez, el primero lo hará de forma silenciosa. Todos los intentos posteriores generan una `ResourceNotFound` excepción.

## 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 los directores adjuntos recuperen, pero no modifiquen, únicamente el contacto BILLING alternativo de una cuenta específica de una organización.

Como `account:AlternateContactTypes` se trata de un tipo de cadena con varios valores, debe utilizar los `ForAnyValue` operadores de cadena [ForAllValuescon varios](#) valores.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "account:GetAlternateContact",
      "Resource": [
        "arn:aws:account::123456789012:account/o-aa111bb222/111111111111"
      ],
      "Condition": {
        "ForAnyValue:StringEquals": {
          "account:AlternateContactTypes": [
            "BILLING"
          ]
        }
      }
    }
  ]
}
```

## Actualiza el contacto principal de tu Cuenta de AWS

Puedes actualizar la información de contacto principal asociada a tu cuenta, incluidos el nombre completo, el nombre de la empresa, la dirección postal, el número de teléfono y la dirección del sitio web del contacto.

El contacto de la cuenta principal se edita 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 contacto de su cuenta principal mediante la consola AWS de administración o mediante AWS CLI y SDK. Para obtener información sobre cómo hacerlo, consulte [Actualizar el contacto principal independiente. Cuenta de AWS](#)
- **Cuentas de AWS dentro de una organización:** en el caso de las cuentas de miembros que forman parte de una AWS organización, un usuario de la cuenta de administración o de la cuenta de administrador delegado puede actualizar de forma centralizada cualquier cuenta de miembro de la organización desde la AWS Organizations consola o mediante programación mediante la AWS CLI y los SDK. Para obtener información sobre cómo hacerlo, consulta [Actualizar el contacto Cuenta de AWS principal](#) de tu organización.

## Temas

- [Requisitos de número de teléfono y dirección de correo electrónico](#)
- [Actualiza el contacto principal para convertirlo en un contacto independiente Cuenta de AWS](#)
- [Actualice el contacto principal de cualquier persona Cuenta de AWS de su organización](#)

## Requisitos de número de teléfono y dirección de correo electrónico

Antes de continuar con la actualización de la información de contacto principal de tu cuenta, te recomendamos que revises primero los siguientes requisitos al introducir números de teléfono y direcciones de correo electrónico.

- Los números de teléfono solo pueden contener números, espacios en blanco y los siguientes caracteres:»». + - ( )
- Los números de teléfono deben comenzar con un código de país + y 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 deben incluir guiones «-» entre el código de área, el código de intercambio y el código local. Por ejemplo, +1 202-555-0179.

### Note

Los números de teléfono ingresados sin guiones pueden provocar que no se puedan recibir llamadas durante el proceso de verificación del número de teléfono al restablecer



un dispositivo MFA para el usuario root. Para obtener más información, consulte [¿Cómo restablezco el dispositivo MFA de mi cuenta de usuario AWS raíz?](#) .

- Por motivos de seguridad, los números de teléfono deben poder recibir SMS desde AWS. No se aceptarán números gratuitos, ya que la mayoría no admiten SMS.
- En el caso de las empresas Cuentas de AWS, se recomienda introducir el número de teléfono y la dirección de correo electrónico de la empresa en lugar de los de una persona física. Configurar el [usuario raíz](#) de la cuenta con la dirección de correo electrónico o el número de teléfono de una persona puede dificultar la recuperación de la cuenta si esa persona deja la empresa.

## Actualiza el contacto principal para convertirlo en un contacto independiente Cuenta de AWS

Para editar sus datos de contacto principales para una versión independiente Cuenta de AWS, lleve a cabo los pasos del siguiente procedimiento. El siguiente AWS Management Console procedimiento siempre funciona solo en el contexto independiente. Puede utilizar el AWS Management Console para acceder o cambiar únicamente la información de contacto principal de la cuenta que utilizó para llamar a la operación.

### AWS Management Console

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 [AWS Management Console](#) como usuario o rol de IAM con los permisos mínimos.
2. Elige el nombre de tu cuenta en la parte superior derecha de la ventana y, a continuación, selecciona Cuenta.

3. Desplázate hacia abajo hasta la sección Información de contacto y, junto a ella, selecciona Editar.
4. Cambie los valores de cualquiera de los campos disponibles.
5. Una vez que haya realizado todos los cambios, elija Actualizar.

## 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 con las cuentas de los miembros, debes [habilitar el acceso confiable al servicio de cuentas](#).

### Permisos mínimos

Para cada operación, debes tener el permiso correspondiente a esa operación:

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

Si utilizas estos permisos individuales, puedes 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.

## Actualice el contacto principal de cualquier persona Cuenta de AWS de su organización

Para editar sus datos de contacto principales Cuenta de AWS en cualquier parte de su organización, lleve a cabo los pasos del siguiente procedimiento.

### Requisitos adicionales

Para actualizar el contacto principal con la AWS Organizations consola, debe realizar algunos ajustes preliminares:

- Su organización debe habilitar todas las funciones para administrar la configuración de las cuentas de sus miembros. Esto permite al administrador controlar las cuentas de los miembros. Esto se establece de forma predeterminada al crear la organización. Si su organización está configurada únicamente para la facturación unificada y desea habilitar todas las funciones, consulte [Habilitar todas las funciones en su organización](#).
- Debe habilitar el acceso confiable al servicio de administración de AWS cuentas. Para configurarlo, consulte [Habilitar el acceso de confianza para la administración de AWS cuentas](#).

## AWS Management Console

Para editar el contacto principal de cualquier miembro Cuenta de AWS de su organización

1. Inicia sesión en la [AWS Organizationsconsola](#) con las credenciales de la cuenta de administración de la organización.
2. Desde Cuentas de AWS, selecciona la cuenta que deseas actualizar.
3. Selecciona Información de contacto y localiza el contacto principal,
4. Seleccione Editar.
5. Cambie los valores de cualquiera de los campos disponibles.
6. Una vez que hayas realizado todos los cambios, selecciona Actualizar.

## 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 con las cuentas de los miembros, debes [habilitar el acceso confiable al servicio de cuentas](#).

- No puedes acceder a una cuenta de una organización diferente a la que utilizas para llamar a la operación.

### Permisos mínimos

Para cada operación, debes tener el permiso correspondiente a esa operación:

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

Si utilizas estos permisos individuales, puedes 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 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 cuentas.

```
$ 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 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 la administración de cuentas.

```
$ 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.

## Actualizar las preguntas sobre desafíos de seguridad

Las preguntas de seguridad son un método de verificación que se utilizaba anteriormente para verificar la identidad en situaciones de recuperación de cuentas. Son menos seguras que las formas de verificación más modernas, como la autenticación multifactorial (MFA). Si actualmente tienes preguntas sobre problemas de seguridad activas en tu cuenta Cuenta de AWS, AWS Support puedes usarlas para autenticarte como propietario de la cuenta.

### Important

A partir del 5 de enero de 2024, ya no AWS se admitirán las preguntas de seguridad para las cuentas que aún no las hayan activado ni utilizado. De este modo, se eliminará la opción de añadir nuevas preguntas de seguridad en la página de cuentas del AWS Management Console. Si ya ha establecido preguntas sobre problemas de seguridad o las ha establecido en la [cuenta de administración](#) de su AWS organización, puede seguir usándolas. A partir del 6 de enero de 2025, ya no AWS admitirá las preguntas sobre problemas de seguridad para el resto de los clientes. Le recomendamos que añada [MFA](#) en su lugar. Para obtener más información, consulta [AWSCuentas suspende el uso de las preguntas sobre problemas de seguridad](#).

Para editar las preguntas de seguridad existentes y proporcionar las respuestas, lleve a cabo los pasos del siguiente procedimiento.

## AWS Management Console

Para editar las preguntas de desafío de seguridad para su Cuenta de AWS

### Permisos mínimos

Para realizar los siguientes pasos, debe tener al menos los siguientes permisos IAM:

- `account:GetChallengeQuestions`(para ver las preguntas sobre los desafíos de seguridad)
- `account:PutChallengeQuestions`(para configurar o actualizar las preguntas de desafío de seguridad)

1. Inicie sesión [AWS Management Console](#) como usuario Usuario raíz de la cuenta de AWS o rol de IAM con los permisos mínimos.
2. Elige el nombre de tu cuenta en la parte superior derecha de la ventana y, a continuación, selecciona Cuenta.
3. Desplázate hacia abajo hasta la sección Preguntas de seguridad y selecciona Editar.

### Note

Si no ves la opción Editar, es probable que no hayas iniciado sesión como usuario root de tu cuenta o como alguien que tenga los permisos mínimos especificados anteriormente.

4. Cambie los valores de cualquiera de los campos disponibles. Puede seleccionar cualquiera de las preguntas proporcionadas y, a continuación, ingresar la respuesta correspondiente.
5. Tras completar los cambios, selecciona Actualizar.

## AWS CLI & SDKs

Esta tarea no es compatible con la AWS CLI o con una operación de API de uno de los AWS SDK. Solamente puede realizar esta tarea mediante la AWS Management Console.

## Especifica qué puede usar Regiones de AWS tu cuenta

Una Región de AWS es una ubicación física en el mundo en la que tenemos varias zonas de disponibilidad. Las zonas de disponibilidad constan de uno o más centros de 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 proporcionan tolerancia a errores, estabilidad y resistencia, y también pueden reducir la latencia. Para ver un mapa de las regiones disponibles y futuras, consulta [Regiones y zonas de disponibilidad](#).

Los recursos que cree en una región no existen en ninguna otra, a menos que utilice explícitamente una función de replicación ofrecida por un AWS servicio. Por ejemplo, Amazon S3 y Amazon EC2 admiten la replicación entre Regiones. Algunos servicios, como AWS Identity and Access Management (IAM), no tienen recursos regionales.

Su cuenta determina las regiones que están disponibles para usted.

- Una Cuenta de AWS proporciona varias regiones para que pueda lanzar AWS recursos en ubicaciones que cumplan con sus requisitos. Por ejemplo, puede que desee lanzar instancias de Amazon EC2 en Europa para estar más cerca de sus clientes europeos o para cumplir con los requisitos legales.
- Una cuenta AWS GovCloud (EE. UU. Oeste) 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 de Amazon AWS (China) solo proporciona acceso a las regiones de Beijing y Ningxia. Para obtener más información, consulte [Amazon Web Services en China](#).

Para obtener una lista de los nombres de las regiones y sus códigos correspondientes, consulte los [puntos finales regionales](#) en la Guía de referencia AWS general. 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 fichas de sesión, estas fichas 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](#).

## Temas

- [Consideraciones antes de activar y desactivar las regiones](#)
- [Habilita o deshabilita una región para cuentas independientes](#)
- [Activa o desactiva una región de tu organización](#)

## Consideraciones antes de activar y desactivar las regiones

Antes de activar o desactivar una región, es importante tener en cuenta lo siguiente:

- Las regiones que se introdujeron antes del 20 de marzo de 2019 están habilitadas de forma predeterminada. Las nuevas están activadas de forma Regiones de AWS predeterminada, lo que significa que puedes empezar a crear y gestionar recursos en estas regiones de forma inmediata. AWS No puedes activar ni desactivar una región que esté habilitada de forma predeterminada. En la actualidad, cuando se AWS añade una región, la nueva región está deshabilitada de forma predeterminada. Si desea que sus usuarios puedan crear y administrar recursos en una nueva región, primero debe habilitar esa región. Las siguientes regiones están deshabilitadas de forma predeterminada.

Nombre	Código
África (Ciudad del Cabo)	af-south-1
Asia-Pacífico (Hong Kong)	ap-east-1

Nombre	Código
Asia-Pacífico (Hyderabad)	ap-south-2
Asia-Pacífico (Yakarta)	ap-southeast-3
Asia-Pacífico (Melbourne)	ap-southeast-4
Canadá (Calgary)	ca-west-1
Europa (Milán)	eu-south-1
Europa (España)	eu-south-2
Europa (Zúrich)	eu-central-2
Israel (Tel Aviv)	il-central-1
Medio Oriente (Baréin)	me-south-1
Medio Oriente (EAU)	me-central-1

- 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 [las políticas de acciones de Billing and Cost Management](#) en la Guía del AWS Billing and Cost Management usuario. También puede utilizar la clave de [aws:RequestedRegion](#) condición para controlar Servicios de AWS el acceso a Región de AWS.
- Habilitar una región es gratis: habilitar una región es gratuito. Solo se te cobrará por los recursos que crees en la nueva región.
- Al deshabilitar una región, se deshabilita el acceso de IAM a los recursos de la región: si inhabilitas una región que aún contiene AWS recursos, como las instancias de Amazon Elastic Compute Cloud (Amazon EC2), pierdes el acceso de IAM a los recursos de esa región. Por ejemplo, no puede utilizarla para ver o AWS Management Console cambiar la configuración de ninguna instancia de EC2 en una región deshabilitada.
- Los cargos por los recursos activos se mantienen si deshabilita una región. Si deshabilita una región que aún contiene AWS recursos, los cargos por esos recursos (si los hubiera) seguirán acumulándose a la tasa estándar. Por ejemplo, si desactiva una región que contiene instancias

de Amazon EC2, tendrá que seguir abonando los cargos por esas instancias, aunque no pueda acceder a ellas.

- La desactivación de una región no siempre está visible de forma inmediata: es posible que los servicios y las consolas estén visibles temporalmente después de deshabilitar una región. La desactivación de una región puede tardar entre unos minutos y varias horas en surtir efecto.
- En algunos casos, la activación de una región lleva de unos minutos a varias horas. Al activar una región, AWS realiza acciones para preparar su cuenta en esa región, como distribuir sus recursos de IAM a la región. Este proceso tarda unos minutos en la mayoría de las cuentas, pero a veces puede tardar varias horas. No puede utilizar la región hasta que este proceso finalice.
- 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 activar o desactivar una región concreta para una cuenta.
- Una sola cuenta puede tener 6 solicitudes de opción de región en curso en un momento dado: una solicitud equivale a habilitar o deshabilitar una región en particular para una cuenta.
- EventBridge Integración con Amazon: los clientes pueden suscribirse a las notificaciones de actualización de estado que opten 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 de optación por región expresivo: debido a la naturaleza asincrónica de habilitar o deshabilitar una región de suscripción voluntaria, hay cuatro posibles estados para una solicitud de suscripción regional:
  - ENABLING
  - DISABLING
  - ENABLED
  - DISABLED

No puedes cancelar una suscripción o exclusión voluntaria si se encuentra en uno de los dos estados. ENABLING DISABLING De lo contrario, ConflictException se lanzará un. 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

- Integración total con AWS Organizations: una cuenta de administración puede modificar o leer la cuenta de cualquier miembro de esa AWS organización. La cuenta de un miembro también puede leer y escribir el estado de su región.

## Habilita o deshabilita 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 AWS Management Console procedimiento siempre funciona solo en el contexto independiente. Puede usarlo AWS Management Console para ver o actualizar solo las regiones disponibles en la cuenta que utilizó para llamar a la operación.

### AWS Management Console

Para habilitar o deshabilitar una región para una región independiente Cuenta de AWS

#### Permisos mínimos

Para realizar los pasos del siguiente procedimiento, un usuario o rol de IAM debe tener los siguientes permisos:

- `account:ListRegions`(necesarios para ver la lista de Regiones de AWS los que están habilitados o deshabilitados actualmente).
- `account:EnableRegion`
- `account:DisableRegion`

1. Inicie sesión [AWS Management Console](#) como usuario Usuario raíz de la cuenta de AWS o rol de IAM con los permisos mínimos.
2. Elige el nombre de tu cuenta en la parte superior derecha de la ventana y, a continuación, selecciona Cuenta.
3. En la página de la cuenta, desplázate hacia abajo hasta la sección Regiones de AWS.

#### Note

Es posible que se te pida que apruebes tu acceso a esta información. AWS envía una solicitud a la dirección de correo electrónico asociada a la cuenta y al número de teléfono de contacto principal. Selecciona el enlace de la solicitud para abrirlo en tu navegador y aprueba el acceso.

4. Junto a cada uno de ellos Región de AWS con una opción en la columna Acción, selecciona Activar o Desactivar, en función de si deseas que los usuarios de tu cuenta puedan crear recursos en esa región y acceder a ellos.

5. Si se te solicita, confirma tu elección.
6. Una vez que haya realizado todos los cambios, elija Actualizar.

## AWS CLI & SDKs

Puedes habilitar, deshabilitar, leer y enumerar el estado de opción de la región mediante los siguientes AWS CLI comandos o sus operaciones equivalentes al AWS SDK:

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

### Permisos mínimos

Para realizar los siguientes pasos, debes 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 leer únicamente la información de su región y conceder a otros la capacidad de leer y escribir.

El siguiente ejemplo habilita una región 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 la administración de cuentas.

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

```
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"
}
```

## Activa o desactiva una región de tu 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 las API de administración de AWS cuentas, de forma que pueda acceder a los datos de las cuentas 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 de una organización para utilizarlas con las cuentas de los miembros, debe:

- Habilite todas las funciones de su organización para administrar la configuración de sus cuentas de miembros. Esto permite al administrador controlar las cuentas de los miembros. Esto se establece de forma predeterminada al crear la organización. Si su organización está configurada únicamente para la facturación unificada y desea habilitar todas las funciones, consulte [Habilitar todas las funciones en su organización](#).
- Habilite el acceso confiable al servicio de administración de AWS cuentas. Para configurarlo, consulte [Habilitar el acceso confiable para la administración de AWS cuentas](#).

## AWS Management Console

Para activar o desactivar una región de su organización

1. Inicie sesión en la AWS Organizations consola con las credenciales de la cuenta de administración de su organización.
2. En la Cuentas de AWS página, selecciona la cuenta que quieres actualizar.
3. Selecciona la pestaña Configuración de la cuenta.
4. En Regiones, selecciona la región que deseas activar o desactivar.
5. Seleccione Acciones y, a continuación, elija la opción Activar o Desactivar.
6. Si ha elegido la opción Activar, revise el texto que se muestra y, a continuación, seleccione Activar región.
7. Si eligió la opción Desactivar, revise el texto mostrado, escriba deshabilitar para confirmar y, a continuación, elija Desactivar 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, debes 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 leer únicamente la información de su región y conceder a otros la capacidad de leer y escribir.

El siguiente ejemplo habilita una región 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 la administración de cuentas.

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

```
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 un `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"
}
```

## Crea o actualiza tu 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, consulte [Crear, eliminar y publicar un Cuenta de AWS alias](#) en la Guía del usuario de IAM.



# Facturación para suCuenta de AWS

Para procedimientos y tareas relacionados con la facturación relacionados con suCuenta de AWS, consulte los siguientes temas en la [AWS Billing and Cost Management](#) [Guía del usuario de](#):

- [Modificación de la moneda utilizada para abonar las facturas](#)
- [Actualización y eliminación de números de identificación fiscal](#)
- [Habilitación de la configuración heredada de impuestos](#)

## Administrar cuentas en India

Si te registras para recibir una nuevaCuenta de AWSy elige India como dirección de contacto, tu acuerdo de usuario es conAmazon Internet Services Private Limited(AISPL), un localAWSun vendedor en la India. AISPL gestiona tu facturación y el total de tu factura aparece en rupias indias (INR) en lugar de en dólares estadounidenses (USD). Una vez creada la cuenta con AISPL, no podrá cambiar el país en la información de contacto.

Si tiene unCuenta de AWScon una dirección en la India, tu cuenta está enAWS o AISPL, según cuándo haya abierto la cuenta. Para saber si tu cuenta está conAWS o AISPL, consulte [Determining which company your account is with](#). Si ya es cliente de AWS, puede seguir utilizando su Cuenta de AWS. También puede optar por tener unCuenta de AWSy una cuenta AISPL, aunque no se pueden consolidar en la mismaAWSorganización. Para obtener información sobre la administración de unCuenta de AWS, consulte [Administre suCuenta de AWS](#).

Si su cuenta pertenece a AISPL, siga los procedimientos de este tema para administrarla. En este tema se explica cómo crear una cuenta AISPL, editar la información sobre su cuenta AISPL y agregar o editar su número de cuenta permanente (PAN).

Como parte de la verificación de la tarjeta de crédito durante el registro, AISPL cargará 2 INR en su tarjeta de crédito. AISPL le reembolsará las 2 INR cuando finalice la verificación. Es posible que se le redirija a su banco como parte del proceso de verificación.

### Temas

- [Determina a qué empresa pertenece tu cuenta](#)
- [Crea unCuenta de AWScon AISPL](#)
- [Administre su cuenta AISPL](#)

## Determina a qué empresa pertenece tu cuenta

Tanto AWS como AISPL prestan servicios de AWS. Siga estos pasos para determinar con qué vendedor tiene su cuenta.

### AWS Management Console

Determinar con qué empresa tiene su cuenta

#### Permisos mínimos

Para realizar los siguientes pasos, debe tener al menos los siguientes permisos de IAM:

- Este procedimiento no requiere permisos especiales.

1. Abra la AWS Management Console en [AWS Management Console](#).
2. En el pie de página, en la parte inferior de la página, consulta el aviso de derechos de autor. Si los derechos de autor son de Amazon Web Services, tiene su cuenta con AWS. Por el contrario, si los derechos de autor son de Amazon Internet Services Private Ltd., tiene su cuenta con AISPL.

### AWS CLI & SDKs

Esta tarea no se admite en el AWS CLI o mediante una operación de API de una de las AWS SDK. Puede realizar esta tarea únicamente mediante el AWS Management Console.

## Crea una Cuenta de AWS con AISPL

AISPL es un vendedor local de AWS en la India. Utilice el procedimiento siguiente para registrarse para obtener una cuenta con AISPL si su dirección de contacto se encuentra en India.

### AWS Management Console

Para registrarse y obtener una cuenta con AISPL

#### Permisos mínimos

Para realizar los siguientes pasos, debe tener al menos los siguientes permisos de IAM:

- Porque esta operación se lleva a cabo antes de que tenga una Cuenta de AWS, esta operación no requiere AWS permisos.

1. Abra el [AWS Management Console](#), a continuación, elija Iniciar sesión en la consola.
2. En la Iniciar sesión página, introduce la dirección de correo electrónico que deseas usar.
3. En su dirección de correo electrónico, seleccione I am a new user y después elija Sign in using our secure server.
4. Para cada uno de los campos de credenciales de inicio de sesión, introduzca su información y, a continuación, elija Crear cuenta.
5. Para cada uno de los campos de información de contacto, introduce tu información.
6. Después de leer el contrato del cliente, seleccione la casilla de verificación de términos y condiciones y, a continuación, elija Create Account and Continue.
7. En la página Payment Information, especifique el medio de pago que desee utilizar.
8. Bajo Información sobre PAN, elige No si no tiene un número de cuenta permanente (PAN) o desea agregarlo más adelante. Si tienes un PAN y quieres añadirlo ahora, elige Sí, y en el SARTÉN introduzca su PAN en el campo.
9. Elija Verify Card and Continue (Verificar tarjeta y continuar). Debe proporcionar su CVV como parte del proceso de verificación. AISPL cargará en su tarjeta 2 INR como parte del proceso de verificación. AISPL le reembolsará las 2 INR cuando finalice la verificación.
10. Para Proporcione un número de teléfono, introduce tu número de teléfono. Si tienes una extensión de teléfono, para Ext, introduce la extensión de tu teléfono.
11. Elija Call Me Now (Llámemme ahora). Después de un momento, aparecerá en pantalla un número de identificación personal de cuatro dígitos.
12. Acepte la llamada automatizada de AISPL. En el teclado del teléfono, introduce el pin de cuatro dígitos que aparece en la pantalla.
13. Cuando la llamada automatizada verifique su número de contacto, seleccione Continue to Select Your Support Plan.
14. En la página Support Plan, seleccione el plan de soporte y, a continuación, elija Continue. Tras verificar tu método de pago y activar tu cuenta, recibirás un mensaje de correo electrónico confirmando la activación de la cuenta.

## AWS CLI & SDKs

Esta tarea no se admite en el AWS CLI o mediante una operación de API de una de las AWS SDK. Puede realizar esta tarea únicamente mediante el AWS Management Console.

## Administre su cuenta AISPL

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. Consulte [Administre su Cuenta de AWS](#).

Utilice el AWS Management Console para realizar las siguientes tareas:

- [Agregar o editar un número de cuenta permanente \(PAN\)](#)
- [Editar varios números de cuenta permanentes \(PAN\)](#)
- [Editar varios números de impuestos sobre bienes y servicios \(GST\)](#)
- [Ver una factura de impuestos](#)

## Cerrar un Cuenta de AWS

Si ya no la necesita Cuenta de AWS, puede cerrarla en cualquier momento siguiendo las instrucciones de esta sección. Una vez que la hayas cerrado, podrás volver a abrirla en un plazo de 90 días a partir del día en que la cerraste. El período comprendido entre el día en que se cerró la cuenta y el momento en que se cierra AWS definitivamente se denomina [período posterior](#) al cierre.

## Lo que necesita 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 de AWS cliente de esta cuenta.
- No es necesario que elimines los recursos de tu 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 en particular, consulte la [AWS documentación](#) correspondiente a ese servicio.
- Puedes volver a abrir tu cuenta durante el período [posterior al cierre](#). Los cargos por los servicios que permanecieron en tu cuenta se reiniciarán si la vuelves a abrir. También sigue siendo responsable de las facturas impagadas y de las [Reserved Instances](#) and [Savings Plans](#) pendientes.

- Usted sigue siendo responsable de todas las comisiones y cargos pendientes por los servicios consumidos antes del cierre de la cuenta. Recibirás una AWS factura al mes siguiente de cerrar tu cuenta. Por ejemplo, si cerraste tu cuenta el 15 de enero, recibirás una factura a principios de febrero por el uso realizado entre el 1 y el 15 de enero. Seguirá recibiendo las facturas de [Reserved Instances](#) and [Savings Plans](#) después de cerrar su cuenta hasta que venzan.
- Ya no podrá acceder a los AWS servicios que antes estaban disponibles en su cuenta. Sin embargo, puedes iniciar sesión y acceder a una cuenta cerrada Cuenta de AWS durante el [período posterior al cierre](#) solo para ver la información de facturación anterior, acceder a la configuración de la cuenta o ponerte en contacto con ella. [AWS Support](#)
- No puedes usar la misma dirección de correo electrónico que tenías registrada Cuenta de AWS en el momento del cierre como correo electrónico principal de otra persona. Cuenta de AWS Si quieres usar la misma dirección de correo electrónico para otra Cuenta de AWS, te recomendamos que la actualices antes del cierre. Consulta las [Actualice el Cuenta de AWS nombre, la dirección de correo electrónico o la contraseña del usuario root](#) instrucciones sobre cómo actualizar tu dirección de correo electrónico.
- Si has [activado la autenticación multifactor \(MFA\)](#) en Cuenta de AWS tu usuario raíz o has configurado un [dispositivo de MFA en un usuario de IAM](#), la MFA no se elimina automáticamente al cerrar la cuenta. Si decides dejar la MFA activada durante los 90 días [posteriores al cierre](#), mantén el dispositivo de MFA activo hasta que finalice el período posterior al cierre en caso de que necesites acceder a la cuenta durante ese tiempo. Tenga en cuenta que los dispositivos con token TOTP de hardware no se pueden asociar a otro usuario tras el cierre permanente de su cuenta. Si desea utilizar el token TOTP de hardware con otro usuario más adelante, tiene la opción de [desactivar el dispositivo MFA](#) de hardware 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 los miembros

- Cuando cierras una cuenta de miembro, esa cuenta no se elimina de la organización hasta después del [período 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 tenga en cuenta para la cuota, consulta [Eliminar una cuenta de miembro de tu organización](#) 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 de cuentas es de 10 y el cierre máximo es de 1000, 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, [cancele primero 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.
- Los dominios registrados con Route 53 no se eliminan automáticamente. Antes de cerrar tu Cuenta de AWS cuenta, tienes cuatro opciones:
  - Puede deshabilitar la renovación automática y los dominios se eliminarán automáticamente cuando venza el período de registro. Para obtener más información, consulte [Habilitación o desactivación de la renovación automática de un dominio](#) en la Guía para desarrolladores de Amazon Route 53.
  - Puede transferir los dominios a otra Cuenta de AWS. Para obtener más información, consulte [Transferir un dominio a otra Cuenta de AWS](#).
  - Puede transferir los dominios a otro registrador de dominios. Para obtener más información, consulte [Transferir un dominio desde Route 53 hacia otro registrador](#).
  - Si ya has cerrado tu cuenta, puedes [abrir un caso AWS Support](#) para obtener ayuda con la transferencia del dominio.

## ¿Cómo cerrar tu cuenta

Puede cerrar la suya 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 tienes algún problema durante el proceso de cierre de tu cuenta, consulta [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 AWS Organizations ella.

Para cerrar una cuenta independiente desde la página de cuentas

1. [Inicie sesión AWS Management Console como usuario raíz](#) en la Cuenta de AWS que desee cerrar. No puedes cerrar una cuenta si has iniciado sesión como usuario o rol de IAM.
2. En la barra de navegación de la esquina superior derecha, elige el nombre o número de tu cuenta y, a continuación, selecciona Cuenta.
3. En la página Cuenta, desplázate hasta la parte inferior de la página hasta la sección Cerrar cuenta. Lee y asegúrate de entender el proceso de cierre de la cuenta.
4. Pulse el botón Cerrar cuenta para iniciar el proceso de cierre de la cuenta.
5. En unos minutos, recibirás un correo electrónico de confirmación de que tu cuenta se ha cerrado.

### Note

Esta tarea no es compatible con una operación de API de uno de los AWS SDK AWS CLI ni con ninguna de ellas. Solo puede realizar esta tarea mediante AWS Management Console

## 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. Las organizaciones que estén en el modo de [facturación unificada](#) no podrán ver el botón Cerrar

en la consola. Para cerrar una cuenta en el modo de facturación unificada, tendrás que seguir los pasos de la pestaña Cuenta independiente.

4. Seleccione cada casilla de verificación para confirmar todas las instrucciones de cierre de cuenta obligatorias.
5. Introduce el ID de la cuenta del miembro y, a continuación, selecciona Cerrar cuenta.

Para cerrar la cuenta de un miembro desde la página de cuentas

Si lo desea, puede cerrar la cuenta de un AWS miembro directamente desde la página de cuentas del AWS Management Console. Para step-by-step obtener orientación, siga las instrucciones de la pestaña Cuenta independiente.

Para cerrar una cuenta de miembro mediante un AWS CLI SDK

Para obtener instrucciones sobre cómo cerrar una cuenta de miembro mediante los SDK AWS CLI y, consulte [Cerrar una cuenta de miembro en su organización en](#) la Guía del AWS Organizations usuario.

## Management account

Una cuenta de administración es Cuenta de AWS aquella que actúa como cuenta principal o raíz de AWS Organizations.

### Note

No puede cerrar una cuenta de administración directamente desde la AWS Organizations consola.

Para cerrar una cuenta de administración desde la página de cuentas

1. [Inicie sesión AWS Management Console como usuario raíz de](#) la cuenta de administración que desee cerrar. No puedes cerrar una cuenta si has iniciado sesión como usuario o rol de IAM.
2. Compruebe que no queden cuentas de miembros activas en su organización. Para ello, ve a la [AWS Organizations consola](#) y asegúrate de que todas las cuentas de los miembros aparezcan Suspended junto a sus nombres de cuenta. Si tienes una cuenta de miembro que sigue activa, tendrás 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 de la esquina superior derecha, elige el nombre o número de tu cuenta y, a continuación, selecciona Cuenta.
4. En la página Cuenta, desplázate hasta la parte inferior de la página hasta la sección Cerrar cuenta. Lee y asegúrate de entender el proceso de cierre de la cuenta.
5. Pulse el botón Cerrar cuenta para iniciar el proceso de cierre de la cuenta.
6. En unos minutos, recibirás un correo electrónico de confirmación de que tu cuenta se ha cerrado.

#### Note

Esta tarea no es compatible con una operación de API de uno de los AWS SDK AWS CLI ni con ninguna de ellas. Solo puede realizar esta tarea mediante AWS Management Console

## 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 la cuenta

Inmediatamente después de cerrar la cuenta, ocurrirá lo siguiente:

- Recibirás un correo electrónico confirmando el cierre de la cuenta en la dirección de correo electrónico del usuario root. 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 SUSPENDED etiqueta junto al nombre de la cuenta en la AWS Organizations consola.

- Si has concedido permisos a otras cuentas para acceder a los servicios de tu Cuenta de AWS cuenta, 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.

## Periodo posterior al cierre

El período posterior al cierre se refiere al período de tiempo transcurrido entre el día en que cerró su cuenta y el momento en que la cierra AWS permanentemente. Cuenta de AWS El período posterior al cierre es de 90 días. Durante el período posterior al cierre, solo podrá acceder a sus contenidos y AWS servicios si vuelve a abrir su 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. Una vez que una cuenta se haya cerrado permanentemente, su [Cuenta de AWS ID](#) 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 tu cuenta antes de que se cierre definitivamente, (1) debes ponerte en contacto contigo lo antes [AWS Support](#) 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.

# Uso de AWS la gestión de cuentas en su organización

AWS Organizations es un AWS servicio que puede utilizar para gestionar Cuentas de AWS su grupo. Esto ofrece funciones como la facturación consolidada, en la que todas las facturas de tus cuentas se agrupan y son gestionadas por un único pagador. También puede gestionar de forma centralizada la seguridad de su organización mediante controles basados en políticas. Para obtener más información sobre AWS Organizations, consulte la [AWS Organizations Guía del usuario de](#) .

## Acceso de confianza

Cuando administra sus cuentas en grupo, la mayoría de las tareas administrativas de la organización solo las puede realizar la cuenta de administración de la organización. AWS Organizations De forma predeterminada, esto incluye solo las operaciones relacionadas con la administración de la propia organización. Puede ampliar esta funcionalidad adicional a otros AWS servicios al habilitar el acceso confiable entre las organizaciones y ese servicio. El acceso confiable otorga permisos al AWS servicio especificado para acceder a la información sobre la organización y las cuentas que contiene. Al habilitar el acceso confiable para la administración de cuentas, el servicio de administración de cuentas otorga a las organizaciones y a sus cuentas de administración permisos para acceder a los metadatos, como la información de contacto principal o alternativa, de todas las cuentas de los miembros de la organización.

Para obtener más información, consulte [Habilitar 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 delegada para la administración de AWS cuentas. Esto permite que la cuenta de administrador delegada realice las mismas tareas de administración de metadatos de administración de cuentas para las cuentas de los miembros de la organización que antes solo podía realizar la cuenta de administración. La cuenta de administrador delegada solo puede acceder a las tareas de administración del servicio de administración de cuentas. La cuenta de administrador delegada no tiene todos los accesos administrativos a la organización que tiene la cuenta de administración.

Para obtener más información, consulte [Habilitar una cuenta de administrador delegado para AWS Administración de cuentas](#).

## Políticas de control de servicios

Cuando Cuenta de AWS forma parte de una organización administrada por AWS Organizations, el administrador de la organización puede aplicar [políticas de control de servicios \(SCP\)](#) que pueden limitar lo que pueden hacer los directores de las cuentas de los miembros. Un SCP nunca concede permisos; en cambio, es un filtro que limita los permisos que puede usar la cuenta del miembro. Un usuario o rol (un principal) de una cuenta de miembro solo puede realizar aquellas operaciones que estén en la intersección de lo que permiten los SCP que se aplican a la cuenta y las políticas de permisos de IAM adjuntas al principal. Por ejemplo, puedes usar los SCP para evitar que el principal de una cuenta modifique los contactos alternativos de su propia cuenta.

Por ejemplo, los SCP que se aplican a Cuentas de AWS, consulte [Restricción del acceso con AWS Organizations Políticas de control de servicios](#).

## Habilitar el acceso confiable para la administración de AWS cuentas

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

Una vez que se haya habilitado el acceso confiable, puede usar el accountID parámetro en las [operaciones de la API de administración de cuentas](#) que lo admiten. Puede utilizar este parámetro correctamente solo si llama a la operación con las credenciales de la cuenta de administración o desde la cuenta de administrador delegada de su organización si habilita una. Para obtener más información, consulte [Habilitar una cuenta de administrador delegado para AWS Administración de cuentas](#).

Utilice el siguiente procedimiento para habilitar el acceso confiable a la administración de cuentas en su organización.

### Permisos mínimos

Para realizar estas tareas, debe cumplir los siguientes requisitos:

- Solo puede hacerlo desde la cuenta de administración de la organización.

- Su organización debe tener [habilitadas todas las características](#).

## AWS Management Console

Para habilitar el acceso confiable a 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. Seleccione Servicios en el panel de navegación.
3. Elija Administración de AWS cuentas en la lista de servicios.
4. Elija Habilitar acceso de confianza.
5. En el cuadro de diálogo Habilitar el acceso confiable para la administración de AWS cuentas, escriba enable para confirmarlo y, a continuación, elija Habilitar el acceso confiable.

## AWS CLI & SDKs

Para habilitar el acceso confiable a la administración de AWS cuentas

Tras ejecutar el siguiente comando, puede utilizar las credenciales de la cuenta de administración de la organización para llamar a las operaciones de la API de administración de cuentas que utilizan el `--accountId` parámetro para hacer referencia a las cuentas de los miembros de una organización.

- AWS CLI: [enable-aws-service-access](#)

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

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

Este comando no genera ningún resultado si se utiliza correctamente.

# Habilitar una cuenta de administrador delegado para AWS Administración de cuentas

Una cuenta de administrador delegado puede llamar a AWS Operaciones de API de administración de cuentas para otras cuentas miembro de la organización. Para designar una cuenta de miembro de su organización como cuenta de administrador delegada, utilice el siguiente procedimiento.

## Permisos mínimos

Para realizar estas tareas, debe cumplir los siguientes requisitos:

- Esto solo se puede realizar desde la cuenta de administración de la organización.
- Su organización debe tener [habilitadas todas las características](#).
- Debe tener [acceso de confianza habilitado para Administración de cuentas en su organización](#).

Después de especificar una cuenta de administrador delegada para su organización, los usuarios y los roles de esa cuenta pueden llamar a AWS CLI y AWS Operaciones del SDK en el `account` espacio de nombres que puede funcionar en el modo Organizations al admitir un `AccountId` parámetro.

## AWS Management Console

Esta tarea no se admite en la AWS Consola de administración de cuentas. Esta tarea solo se puede realizar mediante la AWS CLI o una operación de API de uno de los AWS SDK.

## AWS CLI & SDKs

Para registrar una cuenta de administrador delegado para el servicio de administración de cuentas

Puede utilizar los siguientes comandos para habilitar un administrador delegado para el servicio de administración de cuentas.

Debe especificar la siguiente entidad de servicio:

```
account.amazonaws.com
```

- AWS CLI: [register-delegado-administrador](#)

En el siguiente ejemplo se registra una cuenta de miembro de la organización como administrador delegado del servicio de administración de cuentas.

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

Este comando no genera ninguna salida si se realiza correctamente.

Después de ejecutar este comando, puede utilizar las credenciales de la cuenta 123456789012 para llamar a Administración de cuentasAWS CLIy operaciones de API de SDK que utilizan el `--account-id` para hacer referencia a cuentas miembro de una organización.

## Restricción del acceso conAWS OrganizationsPolíticas de control de servicios

En este tema se presentan ejemplos de cómo puede utilizar políticas de control de servicios (SCP) para restringir lo que pueden hacer los usuarios y las funciones de las cuentas de la organización. Para obtener más información acerca de las políticas de control de servicios, consulte los siguientes temas en laAWS OrganizationsGuía del usuario de:

- [Creación de SCP](#)
- [Adjuntar SCP a unidades organizativas y cuentas](#)
- [Estrategias para SCP](#)
- [Sintaxis de la política SCP](#)

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

En el siguiente ejemplo se niega la `PutAlternateContactyDeleteAlternateContact` Cualquier cuenta de miembro llame a las operaciones de la API en [modo de cuenta independiente](#). Esto evita que cualquier principal de las cuentas afectadas cambie sus propios contactos alternativos.

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

```

        "Sid": "Statement1",
        "Effect": "Deny",
        "Action": [
            "account:PutAlternateContact",
            "account>DeleteAlternateContact"
        ],
        "Resource": [ "arn:aws:account::*:account" ]
    }
]
}

```

Example Ejemplo 2: Evitar que cualquier cuenta de miembro modifique los contactos alternativos de cualquier otra cuenta de miembro de la organización

En el siguiente ejemplo se generaliza el `Resource` elemento a «\*», lo que significa que se aplica a [ambos solicitudes de modo independiente y solicitudes de modo de organización](#). Esto significa que incluso la cuenta de administrador delegado para Administración de cuentas, si el SCP se aplica a ella, no puede cambiar ningún contacto alternativo para cualquier cuenta de la organización.

```

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

```

Example Ejemplo 3: Impedir que una cuenta de miembro en una unidad organizativa modifique sus propios contactos alternativos

El siguiente ejemplo de SCP incluye una condición que compara la ruta de la organización de la cuenta con una lista de dos unidades organizativas. Esto impide que un principal de cualquier cuenta de las unidades organizativas especificadas modifique sus propios contactos alternativos.

```

{

```



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

# Seguridad enAWSAdministración de cuentas

La seguridad en la nube de AWS es la mayor prioridad. Como cliente de AWS, se beneficia de una arquitectura de red y un centro de datos que se han diseñado para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre 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 servicios de AWS en 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 [AWSProgramas de conformidad de](#) . Para obtener más información acerca de los programas de conformidad que se aplican a Administración de cuentas, consulte [Servicios de AWS en el ámbito de aplicación por programa de cumplimiento](#).
- Seguridad en la nube: su responsabilidad viene determinada por el servicio de AWS 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 puede aplicar el modelo de responsabilidad compartida cuando se utilizaAWSAdministración de cuentas. Muestra cómo configurar Administración de cuentas para satisfacer sus objetivos de seguridad y conformidad. También puedes aprender a utilizar otrosAWSque le ayudan a supervisar y proteger los recursos de Administración de cuentas.

## Temas

- [Protección de datos en la gestión de AWS cuentas](#)
- [AWS PrivateLinkparaAWSAdministración de cuentas](#)
- [Identity and Access Management para la administración de AWS cuentas](#)
- [AWSpolíticas gestionadas paraAWSAdministración de cuentas](#)
- [Validación del cumplimiento para la administración de AWS cuentas](#)
- [Resiliencia enAWSAdministración de 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 que ejecuta toda la Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. También es responsable de la configuración de seguridad y de las tareas de administración 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.

Para proteger los datos, recomendamos proteger las credenciales de Cuenta de AWS y configurar cuentas de usuario individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, cada usuario recibe solamente los permisos necesarios para cumplir con sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos de AWS. Se requiere el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad del usuario con AWS CloudTrail.
- Utilizar las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los servicios de Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados FIPS 140-2 al acceder a AWS a través de una interfaz de línea de comandos o una API, utilice un punto de conexión de FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte [Estándar de procesamiento de la información federal \(FIPS\) 140-2](#).

Se recomienda encarecidamente no ingresar información confidencial o sensible, como por ejemplo direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabajas con la administración de cuentas u otro tipo de aplicaciones Servicios de AWS mediante la consola AWS CLI, la API o AWS los SDK. Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres puede ser empleado 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 AWS Administración de cuentas

Si utiliza Amazon Virtual Private Cloud (Amazon VPC) para alojar sus recursos AWS, puede acceder a la Administración de cuentas desde la VPC sin tener que cruzar la Internet pública.

Amazon VPC te permite lanzar recursos AWS de 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 ruteo y las gateways de red. Para obtener más información sobre las VPC, consulte la [Amazon VPC User Guide](#).

Para conectar tu Amazon VPC a Administración de cuentas, primero debes definir un punto de enlace de la VPC de la interfaz, que le permite conectar su VPC a otros servicios AWS. El punto de enlace 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 enlace de la VPC de la interfaz \(AWS PrivateLink\)](#) en la Guía del usuario de Amazon VPC.

### Creación del punto de enlace

Puede crear un endpoint de administración de cuentas en la VPC mediante el AWS Management Console, el AWS Command Line Interface (AWS CLI), un SDK AWS, la API de administración de cuentas, o AWS CloudFormation.

Para obtener información sobre la creación y configuración de un punto de enlace mediante la consola de Amazon VPC o la AWS CLI, consulte [Creación de un punto de enlace de interfaz](#) en la Guía del usuario de Amazon VPC.

#### Note

Al crear un punto de enlace, especifique que Administración de cuentas es el servicio al que desea que se conecte la VPC, utilizando el siguiente formato:

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

Debe utilizar la cadena exactamente como se muestra, especificando la us-east-1 Región. Como servicio global, la administración de cuentas se aloja solo en esa Región.

Para obtener información acerca de cómo se crea y configura un punto de enlace mediante AWS CloudFormation, consulte el recurso [AWS::EC2::VPCEndpoint](#) en la Guía del usuario de AWS CloudFormation.

## Políticas de punto de enlace de Amazon VPC

Puede controlar qué acciones se pueden realizar a través de este endpoint de servicio adjuntando una política de endpoints al crear el endpoint de Amazon VPC. Puede crear reglas de IAM de complejas asociando varias políticas de punto de enlace. Para obtener más información, consulte:

- [Políticas de punto de enlace de Amazon Virtual Private Cloud para Administración de cuentas](#)
- [Control del acceso a los servicios con punto de enlace de la VPC](#) en la AWS PrivateLink Guía.

## Políticas de punto de enlace de Amazon Virtual Private Cloud para Administración de cuentas

Puede crear una política de punto de enlace de Amazon VPC para Administración de cuentas en la que especifique lo siguiente:

- La entidad de seguridad que puede realizar acciones.
- Acciones que los directores pueden realizar.
- El recurso en el que se pueden realizar las acciones.

En el siguiente ejemplo se muestra una política de endpoints de Amazon VPC que permite a un usuario de IAM llamado Alice en la cuenta 123456789012 recuperar y cambiar la información de contacto alternativa para cualquier Cuenta de AWS, pero niega a todos los usuarios de IAM permiso para eliminar cualquier información de contacto alternativa en cualquier cuenta.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "account:GetAlternateContact",
        "account:PutAlternateContact"
      ],
      "Resource": "arn:aws::iam:*:account",
      "Effect": "Allow",
```

```
    "Principal": {
      "AWS": "arn:aws::iam:123456789012:user/Alice"
    },
  ],
  {
    "Action": "account:DeleteAlternateContact",
    "Resource": "*",
    "Effect": "Deny",
    "Principal": "arn:aws::iam:*:root"
  }
]
```

Si desea conceder acceso a las cuentas que forman parte de una AWS Organización a un principal que se encuentra en una de las cuentas de miembro de la organización y, a continuación, el `ResourceElement` debe utilizar el siguiente formato

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

Para obtener más información acerca de la creación de políticas de punto de enlace, consulte [Control del acceso a los servicios con punto de enlace de la VPC](#) en la AWS PrivateLink Guía.

## Identity and Access Management para la administración de AWS cuentas

AWS Identity and Access Management (IAM) es un Servicio de AWS que ayuda a los administradores a controlar de forma segura el acceso a los recursos de AWS. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos de administración de cuentas. IAM es un servicio de Servicio de AWS que se puede utilizar sin cargo adicional.

### Temas

- [Público](#)
- [Autenticación con identidades](#)
- [Administración de acceso mediante políticas](#)
- [Cómo funciona la administración AWS 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 en que se usa AWS Identity and Access Management (IAM) varía según el trabajo que se realice en la administración de cuentas.

Usuario del servicio: si utilizas el servicio de administración de cuentas para realizar tu trabajo, el administrador te proporcionará las credenciales y los permisos que necesitas. A medida que vaya utilizando más funciones de administración de cuentas para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una función de la administración de cuentas, consulte [Solución de problemas AWS de identidad y acceso a la administración de cuentas](#).

Administrador de servicios: si está a cargo de los recursos de administración de cuentas en su empresa, probablemente tenga acceso completo a la administración de cuentas. Es su trabajo determinar a qué funciones y recursos de administración de cuentas deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar la IAM con la administración de cuentas, consulte [Cómo funciona la administración AWS de cuentas con IAM](#).

Administrador de IAM: si es administrador de IAM, puede que desee obtener más información sobre cómo redactar políticas para administrar el acceso a la administración de cuentas. Para ver ejemplos de políticas de administración de cuentas basadas en la identidad que puedes usar en IAM, consulta [Ejemplos de políticas basadas en la identidad para la administración de cuentas AWS](#)

## Autenticación con identidades

La autenticación es la manera de iniciar sesión en AWS mediante credenciales de identidad. Debe estar autenticado (haber iniciado sesión en AWS) como Usuario raíz de la cuenta de AWS, como un usuario de IAM o asumiendo un rol de IAM.

Puede iniciar sesión en AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad de AWS IAM Identity Center. Los usuarios (del IAM Identity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad

federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accede a AWS mediante la federación, está asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en la AWS Management Console o en el portal de acceso a AWS. Para obtener más información sobre el inicio de sesión en AWS, consulte [Cómo iniciar sesión en su Cuenta de AWS](#) en la Guía del usuario de AWS Sign-In.

Si accede a AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de la línea de comandos (CLI) para firmar criptográficamente las solicitudes mediante el uso de las credenciales. Si no utiliza las herramientas de AWS, debe firmar usted mismo las solicitudes. Para obtener más información sobre el método recomendado para la firma de solicitudes, consulte [Firma de solicitudes API de AWS](#) en la Guía del usuario de IAM.

Independientemente del método de autenticación que utilice, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, AWS le recomienda el uso de la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte [Autenticación multifactor](#) en la Guía del usuario de AWS IAM Identity Center y [Uso de la autenticación multifactor \(MFA\) en AWS](#) en la Guía del usuario de IAM.

## Usuario raíz de Cuenta de AWS

Cuando se crea una Cuenta de AWS, se comienza con una identidad de inicio de sesión que tiene acceso completo a todos los recursos y Servicios de AWS de la cuenta. Esta identidad recibe el nombre de usuario raíz de la Cuenta de AWS y se accede a ella iniciando sesión con el email y la contraseña que utilizó para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. 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.

## Identidad federada

Como práctica recomendada, solicite que los usuarios humanos, incluidos los que requieren acceso de administrador, utilicen la federación con un proveedor de identidades para acceder a Servicios de AWS utilizando credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidad web, el AWS Directory Service, el directorio del Identity Center, o cualquier usuario que acceda a Servicios de AWS utilizando credenciales proporcionadas a través de una fuente de



identidad. Cuando identidades federadas acceden a las Cuentas de AWS, asumen roles y los roles proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en el IAM Identity Center o puede conectarse y sincronizar con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus aplicaciones y Cuentas de AWS. Para obtener más información, consulte [¿Qué es el IAM Identity Center?](#) en la Guía del usuario de AWS IAM Identity Center.

## Usuarios y grupos de IAM

Un [usuario de IAM](#) es una identidad en su Cuenta de AWS que dispone de permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte [Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración](#) en la Guía del Usuario de IAM.

Un [grupo de IAM](#) es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte [Cuándo crear un usuario de IAM \(en lugar de un rol\)](#) en la Guía del Usuario de IAM.

## Roles de IAM

Un [rol de IAM](#) es una identidad de tu Cuenta de AWS que dispone de permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente un rol de IAM en la AWS Management Console [cambiando de roles](#). Puede asumir un rol llamando a una operación de AWS CLI o de la API de AWS, o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte [Uso de roles de IAM](#) en la Guía del Usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- **Acceso de usuario federado:** para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte [Creación de un rol para un proveedor de identidades de terceros](#) en la Guía del Usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. El IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte [Conjuntos de permisos](#) en la Guía del usuario de AWS IAM Identity Center.
- **Permisos de usuario de IAM temporales:** un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- **Acceso entre cuentas:** puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. No obstante, con algunos Servicios de AWS se puede asociar una política directamente a un recurso (en lugar de utilizar un rol como representante). Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte [Cómo los roles de IAM difieren de las políticas basadas en recursos](#) en la Guía del usuario de IAM.
- **Acceso entre servicios:** algunos Servicios de AWS utilizan características de otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado a servicios.
- **Reenviar sesiones de acceso (FAS):** cuando utiliza un rol o un usuario de IAM para llevar a cabo acciones en AWS, se le considera una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos de la entidad principal para llamar a un Servicio de AWS, combinados con el Servicio de AWS solicitante para realizar solicitudes a servicios posteriores. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS o recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte [Reenviar sesiones de acceso](#).
- **Rol de servicio:** un rol de servicio es un [rol de IAM](#) que adopta 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 [Creación de un rol para delegar permisos a un Servicio de AWS](#) en la Guía del usuario de IAM.

- Rol vinculado al servicio: un rol vinculado al 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 a servicios aparecen en la 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.
- Aplicaciones que se ejecutan en Amazon EC2: puede utilizar un rol de IAM que le permita administrar credenciales temporales para las aplicaciones que se ejecutan en una instancia de EC2 y realizan solicitudes a la AWS CLI o a la API de AWS. Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia EC2. Para asignar un rol de AWS a una instancia de EC2 y ponerla a disposición de todas las aplicaciones, cree un perfil de instancia asociado a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia EC2 obtener credenciales temporales. Para obtener más información, consulte [Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias de Amazon EC2](#) en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte [Cuándo crear un rol de IAM \(en lugar de un usuario\)](#) en la Guía del usuario de IAM.

## Administración de acceso mediante políticas

Para controlar el acceso en AWS, se crean políticas y se adjuntan a identidades o recursos de AWS. Una política es un objeto de AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando una entidad principal (sesión de rol, usuario o usuario raíz) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan en AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte [Información general de las políticas JSON](#) en la Guía del Usuario de IAM.

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador puede crear políticas de IAM. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con dicha política puede obtener información del rol de la AWS Management Console, la AWS CLI o la API de AWS.

## Políticas basadas en identidades

Las políticas basadas en identidades son documentos de políticas de permisos JSON que puede adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte [Creación de políticas de IAM](#) en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede asociar a varios usuarios, grupos y roles de su Cuenta de AWS. Las políticas administradas incluyen las políticas administradas de AWS y las políticas administradas por el cliente. Para obtener más información sobre cómo elegir una política administrada o una política insertada, consulte [Elegir 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 política JSON que se asocian a un recurso. 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 en función de recursos. Las entidades principales pueden incluir cuentas, usuarios, roles, usuarios federados o Servicios de AWS.

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No se puede utilizar políticas de IAM administradas de AWS en una política basada en recursos.

## Listas de control de acceso (ACL)

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

Amazon S3, AWS WAF y Amazon VPC son ejemplos de servicios que admiten las ACL. Para obtener más información sobre las ACL, consulte [Información general de Lista de control de acceso \(ACL\)](#) en la Guía para Desarrolladores de Amazon Simple Storage Service.

## Otros tipos de políticas

AWS admite otros tipos de políticas adicionales menos frecuentes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- **Límites de permisos:** un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte [Límites de permisos para las entidades de IAM](#) en la Guía del Usuario de IAM.
- **Políticas de control de servicio (SCP):** las SCP son políticas de JSON que especifican los permisos máximos de una organización o una unidad organizativa en AWS Organizations. AWS Organizations es un servicio que le permite agrupar y administrar de manera centralizada varias Cuentas de AWS que posea su empresa. Si habilita todas las características en una empresa, entonces podrá aplicar políticas de control de servicio (SCP) a una o todas sus cuentas. Una SCP limita los permisos para las entidades de las cuentas de miembros, incluido cada Usuario raíz de la cuenta de AWS. Para obtener más información acerca de Organizations y las SCP, consulte [Funcionamiento de las SCP](#) en la Guía del usuario AWS Organizations.
- **Políticas de sesión:** las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para 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 obtener información sobre cómo AWS decide si permite o no una

solicitud cuando hay varios tipos de políticas implicados, consulte [Lógica de evaluación de políticas](#) en la Guía del usuario de IAM.

## Cómo funciona la administración AWS de cuentas con IAM

Antes de usar IAM para administrar el acceso a la administración de cuentas, infórmese sobre las funciones de IAM disponibles para su uso con la administración de cuentas.

Funciones de IAM que puedes usar con la administración de cuentas AWS

Característica de IAM	Soporte de administración de cuentas
<a href="#">Políticas basadas en identidades</a>	Sí
<a href="#">Políticas basadas en recursos</a>	No
<a href="#">Acciones de políticas</a>	Sí
<a href="#">Recursos de políticas</a>	Sí
<a href="#">Claves de condición de políticas</a>	Sí
<a href="#">ACL</a>	No
<a href="#">ABAC (etiquetas en políticas)</a>	Sí
<a href="#">Credenciales temporales</a>	Sí
<a href="#">Permisos de entidades principales</a>	Sí
<a href="#">Roles de servicio</a>	No
<a href="#">Roles vinculados al servicio</a>	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 de gestión de cuentas basadas en la identidad

Compatibilidad con las políticas basadas en identidades      Sí

Las políticas basadas en identidades son documentos de políticas de permisos JSON que puede adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte [Creación de políticas de IAM](#) 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. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para obtener más información sobre los elementos que puede utilizar en una política JSON, consulte [Referencia de los elementos de las políticas JSON de IAM](#) en la Guía del usuario de IAM.

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

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

## Políticas basadas en recursos dentro de la administración de cuentas

Compatibilidad con las políticas basadas en recursos      No

Las políticas basadas en recursos son documentos de políticas JSON que se asocian a un recurso. 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 en función de recursos. Las entidades principales pueden incluir cuentas, usuarios, roles, usuarios federados o servicios de 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. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando la entidad principal y el recurso se encuentran en Cuentas de AWS diferentes, un administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para más información, consulte [Cómo los roles de IAM difieren de las políticas basadas en recursos](#) en la Guía del Usuario de IAM.

## Acciones políticas para la administración de cuentas

Admite acciones de políticas

Sí

Los administradores pueden utilizar las políticas JSON de AWS 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 permitir o denegar el acceso en una política. Las acciones de la política generalmente tienen el mismo nombre que la operación de API de AWS asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

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, consulte [las acciones definidas por la administración de AWS cuentas](#) en la Referencia de autorización de servicios.

Las acciones políticas de la administración de cuentas 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 de administración de cuentas basadas en la identidad, consulte.

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

## Recursos de políticas para la administración de cuentas

Admite recursos de políticas	Sí
------------------------------	----

Los administradores pueden utilizar las políticas JSON de AWS 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. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el [Nombre de recurso de Amazon \(ARN\)](#). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, 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 en el `Resources` elemento de una política de IAM para ayudarle a filtrar la política y distinguir entre estos tipos de Cuentas de AWS:

- `account`

Este resource tipo solo coincide con las cuentas independientes Cuentas de AWS que no son de miembros de una organización gestionada por el AWS Organizations servicio.

- `accountInOrganization`

Este resource tipo solo coincide con Cuentas de AWS las cuentas de los miembros de una organización administrada por el AWS Organizations servicio.

Para ver una lista de los tipos de recursos de administración de cuentas y sus ARN, consulte [los recursos definidos por la administración de AWS cuentas](#) en la Referencia de autorización del servicio. Para saber con qué acciones puede especificar el ARN de cada recurso, consulte [Acciones definidas por la administración de AWS cuentas](#).

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

## Claves de condición de la política para la administración de cuentas

Admite claves de condición de políticas específicas del servicio	Sí
------------------------------------------------------------------	----

Los administradores pueden utilizar las políticas JSON de AWS 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` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen [operadores de condición](#), tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación lógica AND. Si especifica varios valores para una única clave de condición, AWS evalúa la condición con una operación OR lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado

con su nombre de usuario de IAM. Para más información, consulte [Elementos de la política de IAM: variables y etiquetas](#) en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición globales de AWS, consulte [Claves de contexto de condición globales de AWS](#) en la Guía del Usuario de IAM.

El servicio de administración de cuentas admite las siguientes claves de condición que puede utilizar para proporcionar un filtrado detallado a sus políticas de IAM:

- cuenta: TargetRegion

Esta clave de condición utiliza un argumento que consiste en una lista de [códigos de AWS región](#). Permite filtrar la política para que afecte únicamente a 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 que se dirijan a los tipos de contacto alternativos especificados.

- cuenta: AccountResourceOrgPaths

Esta clave de condición utiliza un argumento que consiste en una lista de ARN con caracteres comodín que representan las cuentas de una organización. Permite filtrar la política para que afecte únicamente a las acciones dirigidas a las cuentas con ARN coincidentes. Por ejemplo, el siguiente ARN solo coincide con las cuentas de la organización y la unidad organizativa (OU) especificadas.

```
arn:aws:account::111111111111:ou/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 etiquetas. Permite filtrar la política para que afecte únicamente a las cuentas que son miembros de una organización y que están etiquetadas con las claves y valores de etiqueta especificados.

Para ver una lista de claves de condición de administración de cuentas, consulte [Claves de condición para 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 de administración de cuentas basadas en la identidad, consulte [Ejemplos de políticas basadas en la identidad para la administración de cuentas AWS](#)

## Listas de control de acceso en la administración de cuentas

Admite las ACL

No

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

## Control de acceso basado en atributos con administración de cuentas

Admite ABAC (etiquetas en las políticas)

Sí

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 entidades de IAM (usuarios o roles) y a muchos recursos de AWS. 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 controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el [elemento de condición](#) de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte [¿Qué es ABAC?](#) en la Guía del Usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte [Uso del control de acceso basado en atributos \(ABAC\)](#) en la Guía del Usuario de IAM.

## Uso de credenciales temporales con la administración de cuentas

Admite el uso de credenciales temporales	Sí
------------------------------------------	----

Algunos Servicios de AWS no funcionan cuando inicia sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre qué Servicios de AWS funcionan con credenciales temporales, consulte [Servicios de AWS que funcionan con IAM](#) en la Guía del usuario de IAM.

Utilice credenciales temporales si inicia sesión en la AWS Management Console con cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accede a AWS utilizando el enlace de inicio de sesión único (SSO) de la empresa, ese proceso crea automáticamente credenciales temporales. También crea automáticamente credenciales temporales cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de roles, consulte [Cambio a un rol \(consola\)](#) en la Guía del usuario de IAM.

Puede crear credenciales temporales de forma manual mediante la AWS CLI o la API de AWS. A continuación, puede usar esas credenciales temporales para acceder a AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de usar claves de acceso a largo plazo. Para más información, consulte [Credenciales de seguridad temporales en IAM](#).

## Permisos principales multiservicio para la administración de cuentas

Admite Forward access sessions (FAS)	Sí
--------------------------------------	----

Cuando utiliza un usuario o un rol de IAM para llevar a cabo acciones en AWS, se lo considera una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos de la entidad principal para llamar a un Servicio de AWS, combinados con el Servicio de AWS solicitante para realizar solicitudes a servicios posteriores. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS o recursos para completarse.

En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte [Reenviar sesiones de acceso](#).

## Funciones de servicio para la administración de cuentas

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 [Creación de un rol para delegar permisos a un Servicio de AWS](#) en la Guía del usuario de IAM.

## Funciones vinculadas al servicio para la administración de cuentas

Compatible con roles vinculados al servicio	No
---------------------------------------------	----

Un rol vinculado al 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 a servicios aparecen en la 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, consulte [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 los roles no tienen permiso para crear o modificar los recursos de administración de cuentas. Tampoco pueden realizar tareas mediante la AWS Management Console, la AWS Command Line Interface (AWS CLI) o la API de AWS. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador de IAM puede crear políticas de IAM. A continuación, el administrador puede añadir las políticas de IAM a roles, y los usuarios pueden asumirlos.

Para obtener información sobre cómo crear una política basada en identidad de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte [Creación de políticas de IAM](#) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por la administración de cuentas, incluido el formato de los ARN de cada uno de los tipos de recursos, consulte [las acciones, los recursos y las claves de condición de la administración de AWS cuentas](#) en la Referencia de autorización de servicios.

## Temas

- [Prácticas recomendadas sobre las políticas](#)
- [A través de la página de la cuenta en AWS Management Console](#)
- [Proporcionar acceso de solo lectura a la página de la cuenta en AWS Management Console](#)
- [Proporcionar acceso completo a la página de la cuenta en AWS Management Console](#)

## Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear, acceder o eliminar los recursos de administración de cuentas de su cuenta. Estas acciones pueden generar costes adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas administradas de AWS y continúe con los permisos de privilegio mínimo: a fin de comenzar a conceder permisos a los usuarios y las cargas de trabajo, utilice las políticas administradas de AWS, que conceden permisos para muchos casos de uso comunes. Están disponibles en su Cuenta de AWS. Se recomienda definir políticas administradas por el cliente de AWS específicas para los casos de uso a fin de reducir aún más los permisos. Con el fin de obtener más información, consulte las [políticas administradas por AWS](#) o las [políticas administradas por AWS para funciones de trabajo](#) en la Guía del 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 de 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 puede usar condiciones para conceder acceso a acciones de servicios si se emplean a través de un Servicio de AWS determinado, como por ejemplo AWS CloudFormation. Para obtener más información, consulte [Elementos de la política de JSON de IAM: Condición](#) en la Guía del usuario de IAM.

- Utilice 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. xPara más información, consulte la [política de validación del Analizador de acceso de IAM](#) en la Guía de usuario de IAM.
- Solicite la autenticación multifactor (MFA): si se encuentra en una situación en la que necesita usuarios raíz o de IAM en su Cuenta de AWS, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para obtener más información, consulte [Configuración de acceso a una API protegida por MFA](#) en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las [Prácticas recomendadas de seguridad en IAM](#) en la Guía del usuario de IAM.

## A través de la página de la cuenta en AWS Management Console

Para acceder a la página de la cuenta en AWS Management Console, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre su Cuenta de AWS. Si crea una política basada en identidad que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles de IAM) que tengan esa política.

Para garantizar que los usuarios y los roles puedan usar la consola de administración de cuentas, puede optar por adjuntar la política `AWSAccountManagementFullAccess` AWS gestionada `AWSAccountManagementReadOnlyAccess` o la política gestionada a las entidades. Para obtener más información, consulte [Adición de permisos a un usuario](#) en la Guía del usuario de IAM.

No es necesario que conceda permisos mínimos para la consola a los usuarios que solo realizan llamadas a AWS CLI o a la API de AWS. En cambio, en muchos casos, puedes optar por permitir el acceso solo a las acciones que coincidan con las operaciones de la API que intentas realizar.



## Proporcionar acceso de solo lectura a la página de la cuenta en AWS Management Console

En el siguiente ejemplo, desea conceder a un usuario de IAM acceso de Cuenta de AWS solo lectura a la página de la cuenta del. AWS Management Console Los usuarios con esta política adjunta no pueden realizar ningún cambio.

La `account:GetAccountInformation` acción permite acceder a la mayoría de los ajustes de la página de la cuenta. Sin embargo, para ver las AWS regiones actualmente habilitadas, también debes incluir la `account:ListRegions` acción.

```
{
  "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 AWS Management Console

En el siguiente ejemplo, desea conceder a un usuario de IAM acceso Cuenta de AWS completo a la página de la cuenta delAWS Management Console. Los usuarios con esta política adjunta pueden modificar la configuración de la cuenta.

Esta política de ejemplo se basa en la política del ejemplo anterior y agrega cada uno de 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.

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

```
{
  "Sid": "GrantFullAccessToAccountSettings",
  "Effect": "Allow",
  "Action": [
    "account:GetAccountInformation",
    "account:ListRegions",
    "account:PutContactInformation",
    "account:PutChallengeQuestions",
    "account:PutAlternateContact",
    "account>DeleteAlternateContact",
    "account:EnableRegion",
    "account:DisableRegion"
  ],
  "Resource": "*"
}
```

## Uso de políticas basadas en la identidad (políticas de IAM) para la administración de cuentas AWS

Para obtener información detallada acerca de las cuentas de AWS y los usuarios de IAM, consulte [¿Qué es 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 administradas por el cliente \(consola\)](#) en la Guía del usuario de IAM.


### AWSPolíticas de acciones de administración de cuentas

En esta tabla se resumen los permisos que permiten el acceso a la configuración de tu cuenta. Para ver ejemplos de políticas que utilizan estos permisos, consulta los [ejemplos de políticas de administración de AWS cuentas](#).


#### Note

Para conceder a los usuarios de IAM acceso de escritura a una configuración de [cuenta específica en la página Cuenta](#) del usuarioAWS Management Console, debe conceder el `GetAccountInformation` permiso, además del permiso (o los permisos) que desee utilizar para modificar esa configuración.

Nombre del permiso	Nivel de acceso	Descripción
<code>account:ListRegions</code>	Enumeración	Otorga permiso para enumerar las regiones disponibles.
<code>account:GetAccountInformation</code>	Leer	Otorga permiso para recuperar la información de una cuenta.
<code>account:GetAlternateContact</code>	Leer	Otorga permiso para recuperar los contactos alternativos de una cuenta.
<code>account:GetChallengeQuestions</code>	Leer	Otorga permiso para recuperar las preguntas de desafío de una cuenta.
<code>account:GetContactInformation</code>	Leer	Otorga permiso para recuperar la información de contacto principal de una cuenta.
<code>account:GetRegionOptStatus</code>	Leer	Otorga permiso para obtener el estado de suscripción de una región.
<code>account:CloseAccount</code>	Escritura	Otorga permiso para cerrar una cuenta.

 **Note**

Este es un permiso solo para la consola. No hay acceso de API disponible para este permiso.

Nombre del permiso	Nivel de acceso	Descripción
<code>account:DeleteAlternateContact</code>	Escritura	Otorga permiso para eliminar los contactos alternativos de una cuenta.
<code>account:DisableRegion</code>	Escritura	Otorga permiso para deshabilitar el uso de una región.
<code>account:EnableRegion</code>	Escritura	Otorga permiso para permitir el uso de una región.
<code>account:PutAlternateContact</code>	Escritura	Otorga permiso para modificar los contactos alternativos de una cuenta.
<code>account:PutChallengeQuestions</code>	Escritura	Otorga permiso para modificar las preguntas de desafío de una cuenta.  <div data-bbox="1068 1010 1507 1373" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"> <p> <b>Note</b></p> <p>Este es un permiso solo para la consola. No hay acceso de API disponible para este permiso.</p> </div>
<code>account:PutContactInformation</code>	Escritura	Otorga permiso para actualizar la información de contacto principal de una cuenta.

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

Usa la siguiente información para ayudarte a diagnosticar y solucionar los problemas más comunes que pueden surgir al trabajar con la administración de cuentas y la IAM.

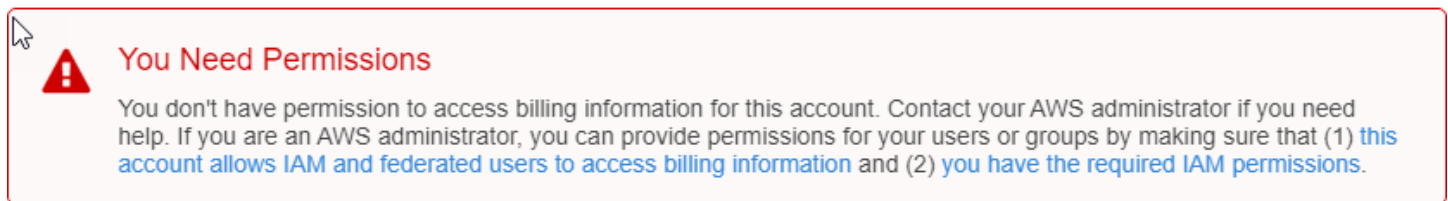
## Temas

- [No estoy autorizado a realizar ninguna 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 estoy autorizado a realizar ninguna acción en la página de la cuenta

Si la AWS Management Console le indica que no está autorizado para llevar a cabo una acción, debe ponerse en contacto con su administrador para recibir ayuda. Su administrador es la persona que le facilitó su nombre de usuario y 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 la cuentaAWS Management Console, pero no tiene los `account:GetAccountInformation` permisos necesarios.



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 recibes un mensaje de error que indica que no estás autorizado a realizar la `iam:PassRole` acción, debes actualizar tus políticas para que puedas transferir una función a la administración de cuentas.

Algunos Servicios de AWS le permiten transferir un rol existente a dicho servicio en lugar de crear un nuevo rol de servicio o uno vinculado al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

El siguiente ejemplo de error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en la administración de cuentas. Sin embargo, la acción requiere que el servicio cuente con permisos que concede 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 administrador de AWS. 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

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para saber si la administración de cuentas admite estas funciones, consulte [Cómo funciona la administración AWS de cuentas con IAM](#).
- Para obtener información acerca de cómo proporcionar acceso a los recursos de las Cuentas de AWS de su propiedad, consulte [Proporcionar acceso a un usuario de IAM a otra Cuenta de AWS de la que es propietario](#) en la Guía del usuario de IAM.
- Para obtener información acerca de cómo proporcionar acceso a tus recursos a Cuentas de AWS de terceros, consulte [Proporcionar acceso a Cuentas de AWS que son propiedad de terceros](#) en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante federación de identidades, consulte [Proporcionar acceso a usuarios autenticados externamente \(federación de identidades\)](#) en la Guía del usuario de IAM.
- Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte [Cómo los roles de IAM difieren de las políticas basadas en recursos](#) en la Guía del Usuario de IAM.

# AWS políticas gestionadas para AWS Administración de cuentas

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

- [Política administrada por AWS: AWSAccountManagementReadOnlyAccess](#)
- [Política administrada por AWS: AWSAccountManagementFullAccess](#)
- [Actualizaciones de administración de cuentas para AWS políticas gestionadas](#)

Una política administrada de AWS es una política independiente que AWS crea y administra. Las políticas administradas de AWS se diseñan para ofrecer permisos para muchos casos de uso comunes, por lo que puede empezar a asignar permisos a los usuarios, grupos y roles.

Tenga presente que es posible que las políticas administradas de AWS no concedan permisos de privilegio mínimo para los casos de uso concretos, ya que están disponibles para que las utilicen todos los clientes de AWS. Se recomienda definir [políticas administradas por el cliente](#) para los casos de uso a fin de reducir aún más los permisos.

No puede cambiar los permisos definidos en las políticas administradas por AWS. Si AWS actualiza los permisos definidos en una política administrada de AWS, la actualización afecta a todas las identidades de entidades principales (usuarios, grupos y roles) a las que está adjunta la política. Lo más probable es que AWS actualice una política administrada de AWS cuando se lance un nuevo Servicio de AWS o las operaciones de la API nuevas estén disponibles para los servicios existentes.

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

## Política administrada por AWS: AWSAccountManagementReadOnlyAccess

Puede adjuntar la política `AWSAccountManagementReadOnlyAccess` a las identidades de IAM.

Esta política proporciona permisos de solo lectura para ver solo lo siguiente:

- Los metadatos sobre su Cuentas de AWS
- El Regiones de AWS que están habilitados o deshabilitados para Cuenta de AWS (solo puede ver el estado de las regiones en su cuenta mediante el AWS consola)

Para ello, concede permiso para ejecutar cualquiera de los `Get` o `List` operaciones. No ofrece ninguna posibilidad de modificar los metadatos de la cuenta ni de habilitar o deshabilitar Regiones de AWS para la cuenta.

### Detalles de los permisos

Esta política incluye los siguientes permisos.

- `account`— Permite a los directores recuperar la información de metadatos sobre Cuentas de AWS. También permite a los directores enumerar los Regiones de AWS que están habilitadas para la cuenta en AWS Management Console.

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

## Política administrada por AWS: `AWSAccountManagementFullAccess`

Puede adjuntar 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
- El Regiones de AWS que están habilitados o deshabilitados para Cuenta de AWS (solo puede ver el estado o habilitar o deshabilitar Regions en su cuenta mediante el AWS consola)

Para ello, concede permiso para ejecutar cualquier `account` operaciones.

### 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 los directores enumerar los Regiones de AWS que estén habilitadas para la cuenta y que las habiliten o deshabiliten en AWS Management Console.

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

## Actualizaciones de administración de cuentas para AWS políticas gestionadas

Ver detalles sobre las actualizaciones de AWS políticas administradas para la administración de cuentas desde que este servicio comenzó a rastrear estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbese a la fuente RSS de la página del historial de documentos de administración de cuentas.

Cambio	Descripción	Fecha
AWS La administración de cuentas se lanzó con la nueva AWS administró políticas y comenzó a rastrear los cambios	La administración de cuentas se lanzó inicialmente con lo siguiente AWS políticas gestionadas: <ul style="list-style-type: none"> <li>• <a href="#">AWSAccountManageme ntReadOnlyAccess</a></li> <li>• <a href="#">AWSAccountManageme ntFullAccess</a></li> </ul>	30 de septiembre de 2021

# Validación del cumplimiento para la administración de AWS cuentas

Los auditores externos evalúan la seguridad y el cumplimiento de AWS los servicios que se pueden ejecutar en su Cuenta de AWS empresa como parte de varios programas de AWS cumplimiento. Estos incluyen SOC, PCI, FedRAMP, HIPAA y otros.

Para obtener una lista de AWS los servicios incluidos en el ámbito de programas de cumplimiento específicos, consulte [Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS](#) . Para obtener información general, consulte [Programas de conformidad de AWS](#).

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

Su responsabilidad de cumplimiento al utilizar los servicios de su empresa Cuenta de AWS está 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 facilitar el cumplimiento:

- [Guías de inicio rápido de seguridad y conformidad](#): estas guías de implementación tratan consideraciones sobre arquitectura y ofrecen pasos para implementar los entornos de referencia centrados en la seguridad y la conformidad en AWS.
- [Architecting for HIPAA Security and Compliance on Amazon Web Services](#) (Arquitectura para la seguridad y el cumplimiento de la HIPAA en Amazon Web Services): en este documento técnico, se describe cómo las empresas pueden utilizar AWS para crear aplicaciones aptas para HIPAA.

## Note

No todos los Servicios de AWS son aptos para HIPAA. Para obtener más información, consulte la [Referencia de servicios aptos para HIPAA](#).

- [Recursos de conformidad de AWS](#): este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- [Evaluación de recursos con reglas](#) en la Guía para desarrolladores de AWS Config: el servicio AWS Config evalúa en qué medida las configuraciones de sus recursos cumplen las prácticas internas, las directrices del sector y las normativas.

- [AWS Security Hub](#): este Servicio de AWS proporciona una vista integral de su estado de seguridad en AWS que lo ayuda a verificar la conformidad con los estándares y las prácticas recomendadas del sector de seguridad.
- [AWS Audit Manager](#): este Servicio de AWS le ayuda a auditar continuamente el uso de AWS con el fin de simplificar la forma en que administra el riesgo y la conformidad con las normativas y los estándares del sector.

## Resiliencia en AWS Administración de cuentas

La infraestructura global de AWS se basa en regiones de AWS y zonas de disponibilidad de AWS. 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 latencia. 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 centros de datos únicos o múltiples.

Para obtener más información sobre las Regiones de AWS y las zonas de disponibilidad, consulte [Infraestructura global de AWS](#).

## Seguridad de la infraestructura en AWS Account Management

Como servicios gestionados, los servicios que se ejecutan en su Cuenta de AWS empresa están protegidos por la seguridad de la red AWS global. Para obtener información sobre los servicios de seguridad de AWS y cómo AWS protege la infraestructura, consulte [Seguridad en la nube de AWS](#). Para diseñar su entorno de AWS con las prácticas recomendadas de seguridad de infraestructura, consulte [Protección de la infraestructura](#) en Portal de seguridad de AWS Well-Architected Framework.

Las llamadas a la API AWS publicadas se utilizan para acceder a la configuración de la cuenta a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS) Nosotros exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) tales 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 de seguridad de IAM. También puede utilizar [AWS Security Token Service](#) (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

# Supervisión de la gestión de AWS cuentas

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 depósito de Amazon Simple Storage Service (Amazon S3) que especifique. Esto le permite identificar qué usuarios y cuentas llamaron a AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. 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 en los recursos. Los eventos de AWS los servicios se entregan EventBridge prácticamente en tiempo real. Puede crear reglas sencillas para indicar qué eventos le resultan de interés, así como qué acciones automatizadas se van a realizar cuando un evento cumple una de las reglas. Para obtener más información, consulta la [Guía del EventBridge usuario de Amazon](#).

## Registro de AWS Llamadas a la API de Account Management AWS CloudTrail

Las API de administración de cuentas están integradas con AWS CloudTrail, un servicio que proporciona un registro de las acciones que realiza un usuario, un rol o un AWS servicio que llama a una operación de administración de cuentas. CloudTrail captura todas las llamadas a la API de Account Management como eventos. Las llamadas capturadas incluyen todas las llamadas a las operaciones de administración de cuentas. Si crea un registro de seguimiento, puede activar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3, incluidos los eventos de Account Management (Administración de cuentas). Si no configura un registro de seguimiento, puede ver los eventos más recientes de la consola de CloudTrail en el Event history (Historial de eventos). Mediante la información que recopila por CloudTrail, se puede determinar la solicitud que denominó una operación de Administración de cuentas, la dirección IP utilizada para realizar la solicitud, quién la realizó y cuándo, etc.

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

## Información de Administración de cuentas en CloudTrail

CloudTrail se habilita en el Cuenta de AWS cuando crea la cuenta de. Cuando se produce una actividad de mediante una operación de Administración de cuentas, CloudTrail registra esa actividad en un evento de CloudTrail junto con los demás AWS eventos de servicio de en Historial de eventos. Puede ver, buscar y descargar los últimos eventos de la Cuenta de AWS. Para obtener más información, consulte [Ver eventos con el historial de eventos de CloudTrail](#).

Para mantener un registro continuo de los eventos de Cuenta de AWS, incluidos los eventos de las operaciones de Administración de cuentas, cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la AWS Management Console, el rastro se aplica a todas las 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. También puede configurar otros servicios de AWS para analizar y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte los siguientes:

- [Introducción a la creación de registros de seguimiento](#)
- [Servicios e integraciones compatibles con CloudTrail](#)
- [Configuración de notificaciones de Amazon SNS para CloudTrail](#)
- [Recepción de archivos de registro de CloudTrail de varias regiones](#)
- [Recepción de archivos de registro de CloudTrail de varias cuentas](#)

AWS CloudTrail registra todas las operaciones de API de administración de cuentas encontradas en el [Referencia de la API](#) sección de esta guía. Por ejemplo, las llamadas a las operaciones `CreateAccount`, `DeleteAlternateContact` y `PutAlternateContact` generan entradas en los archivos de registro de CloudTrail.

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 el usuario raíz o AWS Identity and Access Management credenciales de usuario (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 de AWS.

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

## Descripción de las entradas de registro de administración de cuentas

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registros en un bucket de Amazon S3 que especifique. Los archivos log de CloudTrail pueden contener una o varias entradas de log. Un evento representa una única solicitud de cualquier origen e incluye información sobre la operación solicitada, la fecha y la hora de la operación, los parámetros de la solicitud, etcétera. Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas públicas a la API, por lo que estas no aparecen en ningún orden específico.

Ejemplo 1: En el siguiente ejemplo, se muestra una entrada del registro de CloudTrail para una llamada a la `GetAlternateContact` operación para recuperar la corriente `OPERATIONScontacto` alternativo para 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: En el siguiente ejemplo, se muestra una entrada del registro de CloudTrail para una llamada a la `PutAlternateContact` operación para agregar un nuevo `BILLING` contacto 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: En el siguiente ejemplo, se muestra una entrada del registro de CloudTrail para una llamada a la `DeleteAlternateContact` operación para eliminar el actual `OPERATIONS` contacto alternativo.

```

{
  "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": "AROAI234567890EXAMPLE",
    "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
    "accountId": "123456789012",
    "userName": "ServiceTestRole"
  },
  "webIdFederationData": {},
  "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2021-04-30T18:33:00Z"
  }
}
},
"eventTime": "2021-04-30T18:33:16Z",
"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 específicas 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 administración de cuentas

En los siguientes ejemplos se muestran los eventos de la administración de cuentas. Los eventos se producen en la medida de lo posible.

Actualmente, solo los eventos específicos para habilitar o deshabilitar las regiones y las llamadas a la API mediante regiones CloudTrail están disponibles para la administración de cuentas.

Event types (Tipos de eventos)

- [Evento para activar y desactivar regiones](#)

### Evento para activar y desactivar regiones

Al activar o desactivar 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 una de 2020-09-30 las ap-east-1 regiones era una cuenta123456789012.

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

```
}  
}
```

Hay cuatro estados posibles que coinciden con los estados devueltos por las API `GetRegionOptStatus` y `ListRegions`:

- **ENABLED**— La región se ha habilitado correctamente para lo indicado `accountId`
- **ENABLING**— La región está en proceso de habilitarse para lo `accountId` indicado
- **DISABLED**— La región se ha desactivado correctamente para lo `accountId` indicado
- **DISABLING**— La región está en proceso de ser deshabilitada para lo `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 **ENABLED** los eventos de una **DISABLED** región.

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

# Referencia de la API

Las operaciones de la API en la gestión de cuentas (account) el espacio de nombres le permite modificar su Cuenta de AWS.

Cada Cuenta de AWS admite metadatos con información sobre la cuenta, incluida información sobre hasta tres contactos alternativos asociados a la cuenta. Estos datos se suman a la dirección de correo electrónico asociada a la [usuario root](#) de la cuenta. Solo puede especificar uno de cada 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. El [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. Alternativamente, puede llamar a estas operaciones de API desde una identidad en un [AWS Organizations](#) cuenta de administración y especifique el número de identificación de la cuenta de cualquier Cuenta de AWS que es miembro de la organización.

## Versión de API

Esta versión de la referencia de la API de cuentas documenta la versión de la API de administración de cuentas 2021-02-01.

### Note

Como alternativa al uso directo de la API, puede utilizar una de las [AWS SDK](#), que constan de bibliotecas y código de muestra para varios lenguajes de programación y plataformas (Java, Ruby, .NET, iOS, Android y más). Los SDK proporcionan una forma cómoda de crear un acceso programático a [AWS Organizations](#). Por ejemplo, los SDK se encargan de firmar criptográficamente las solicitudes, gestionar los errores y reintentar las solicitudes automáticamente. Para obtener más información acerca de los SDK de AWS, incluido cómo descargarlos e instalarlos, consulte [Herramientas para Amazon Web Services](#).

Le recomendamos que utilice elAWSSDK para realizar llamadas programáticas a la API al servicio de administración de cuentas. Sin embargo, también puedes usar la API de consultas de administración de cuentas para realizar llamadas directas al servicio web de administración de cuentas. Para obtener más información sobre la API de consultas de administración de cuentas, consulte [Llamar a la API mediante solicitudes de consulta HTTP](#) en la Guía del usuario de administración de cuentas. Las organizaciones admiten las 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 operaciones que requieran tamaños más grandes, utilice una solicitud POST.

## Firma de solicitudes

Al enviar solicitudes HTTP aAWS, debe firmar las solicitudes para queAWSpueda identificar quién los envió. Firmas las solicitudes con tusAWSclave de acceso, que consiste en un identificador de clave de acceso y una clave de acceso secreta. Le recomendamos encarecidamente que no cree una clave de acceso para su cuenta raíz. Cualquier persona que tenga la clave de acceso a su cuenta raíz tiene acceso sin restricciones a todos los recursos de su cuenta. En su lugar, cree una clave de acceso para un usuario de IAM que tenga privilegios administrativos. Como otra opción, utiliceAWSSecurity Token Service para generar credenciales de seguridad temporales y utilizarlas para firmar solicitudes.

Para firmar solicitudes, te recomendamos que utilices la versión 4 de Signature. Si ya tiene una aplicación que usa la versión 2 de Signature, no es necesario que la actualice para usar la versión 4 de Signature. Sin embargo, algunas operaciones ahora requieren la versión 4 de Signature. La documentación de las operaciones que requieren la versión 4 indica este requisito. Para obtener más información, consulte [Firma de solicitudes de API de AWS](#) en la Guía del usuario de IAM.

Cuando usa elAWSInterfaz de línea de comandos (AWSCLI) o una de lasAWSSDK a los que realizar solicitudesAWS, estas herramientas firman automáticamente las solicitudes por usted con la clave de acceso que especifique al configurar las herramientas.

## Soporte y comentarios para la administración de cuentas

Agradecemos sus comentarios. Envíe sus comentarios a [feedback-awsaccounts@amazon.com](mailto:feedback-awsaccounts@amazon.com) publique sus comentarios y preguntas en [Foro de soporte de administración de cuentas](#). Para obtener más información acerca de los foros de soporte de AWS, consulte la [Ayuda de los foros](#).

## Cómo se presentan los ejemplos

El JSON devuelto por la administración de cuentas 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. Cuando 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 debes enviar la entrada como una cadena de texto JSON única.

## Grabación de solicitudes de API

Soportes de administración de cuentas CloudTrail, un servicio que graba AWS La API llama para su Cuenta de AWS y entrega los archivos de registro a un bucket de Amazon S3. Mediante el uso de la información recopilada por CloudTrail, puede determinar qué solicitudes se realizaron correctamente a Account Management, quién hizo la solicitud, cuándo se hizo, etc. Para obtener más información sobre la administración de cuentas y su soporte para CloudTrail, consulte [Registro de AWS Llamadas a la API de Account Management AWS CloudTrail](#). Para obtener más información sobre CloudTrail, incluida la forma de activarlo y buscar los archivos de registro, consulte la [AWS CloudTrail Guía del usuario](#).

## Acciones

Se admiten las siguientes acciones:

- [DeleteAlternateContact](#)
- [DisableRegion](#)
- [EnableRegion](#)
- [GetAlternateContact](#)
- [GetContactInformation](#)
- [GetRegionOptStatus](#)
- [ListRegions](#)
- [PutAlternateContact](#)
- [PutContactInformation](#)

## DeleteAlternateContact

Elimina el contacto alternativo especificado de un Cuenta de AWS.

Para obtener detalles completos sobre cómo utilizar las operaciones de contacto alternativas, consulte [Acceder a los contactos alternativos o actualizarlos](#).

### 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 [Habilitar el acceso confiable para la administración de AWS cuentas](#).

## 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 de la misma organización. La organización debe tener [todas las funciones habilitadas](#) y debe tener habilitado el [acceso de confianza](#) para el servicio de administración de cuentas y, si lo desea, debe tener asignada una cuenta de [administrador delegado](#).

 Note

La cuenta de administración no puede especificar la suya propia `AccountId`; debe llamar a la operación en un contexto independiente sin incluir el `AccountId` parámetro.

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 desee recuperar o modificar.

Tipo: String

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 produjo un error en la operación porque la identidad que realiza la llamada no tiene los permisos mínimos necesarios.

Código de estado HTTP: 403

### InternalServerErrorException

La operación falló debido a un error interno deAWS. Vuelva a intentar la operación más tarde.

Código de estado HTTP: 500

### ResourceNotFoundException

La operación falló porque especificó un recurso que no se encuentra.

Código de estado HTTP: 404

### TooManyRequestsException

Se produjo un error en la operación porque se llamaba con demasiada frecuencia y se había superado el límite establecido.

Código de estado HTTP: 429

### ValidationException

La operación falló porque uno de los parámetros de entrada no era válido.

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

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

## 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 administración de cuentas.

## 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 los SDK de AWS de un lenguaje específico, consulte:

- [Interfaz de la línea de comandos de AWS](#)
- [SDK de AWS para .NET](#)
- [SDK de AWS para C++](#)
- [SDK de AWS para Go](#)

- [SDK de AWS para Java V2](#)
- [AWSSDK para la versión 3 JavaScript](#)
- [SDK de AWS para PHP V3](#)
- [SDK de AWS para Python](#)
- [SDK de AWS para Ruby V3](#)

# DisableRegion

Inhabilita (excluye) una región determinada de una cuenta.

## Note

Al deshabilitar una región, se 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 el Cuenta de AWS 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 también debe ser una cuenta de miembro de la misma organización. La organización debe tener [todas las funciones habilitadas](#) y debe tener habilitado el [acceso de confianza](#) para el servicio de administración de cuentas y, si lo desea, debe tener asignada una cuenta de [administrador delegado](#).

**Note**

La cuenta de administración no puede especificar la suya propia. AccountId Debe llamar a la operación en un contexto independiente sin incluir el AccountId parámetro.

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

Tipo: String

Patrón: `^\d{12}$`

Obligatorio: no

### RegionName

Especifica el código de región de un nombre de región determinado (por ejemplo, `af-south-1`). Cuando inhabilitas una región, AWS realiza acciones para desactivarla en tu 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 podrá activar la región hasta que el proceso de desactivación haya finalizado por completo.

Tipo: string

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 produjo un error en la operación porque la identidad que realiza la llamada no tiene los permisos mínimos necesarios.

Código de estado HTTP: 403

### ConflictException

No se pudo procesar la solicitud debido a un conflicto en el estado actual del recurso. Por ejemplo, esto ocurre si intenta habilitar una región que está actualmente deshabilitada (en estado DESHABILITADO).

Código de estado HTTP: 409

### InternalServerError

La operación falló debido a un error interno de AWS. Vuelva a intentar la operación más tarde.

Código de estado HTTP: 500

### TooManyRequestsException

La operación falló porque se realizó con demasiada frecuencia y superó el límite de aceleración.

Código de estado HTTP: 429

### ValidationException

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

Código de estado HTTP: 400

## Véase también

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

- [Interfaz de la línea de comandos de AWS](#)

- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)



# EnableRegion

Habilita (habilita) una región determinada 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 el Cuenta de AWS 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 también debe ser una cuenta de miembro de la misma organización. La organización debe tener [todas las funciones habilitadas](#) y debe tener habilitado el [acceso de confianza](#) para el servicio de administración de cuentas y, si lo desea, debe tener asignada una cuenta de [administrador delegado](#).

#### Note

La cuenta de administración no puede especificar la suya propia. AccountId Debe llamar a la operación en un contexto independiente sin incluir el AccountId parámetro.

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

Tipo: String

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 en la mayoría de las cuentas, pero puede tardar varias horas. No puede utilizar la región hasta que este proceso finalice. Además, no puedes deshabilitar la región hasta que el proceso de activación se haya completado 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

La operación falló porque la identidad que realiza la llamada no tiene los permisos mínimos requeridos.

Código de estado HTTP: 403

## ConflictException

No se pudo procesar la solicitud debido a un conflicto en el estado actual del recurso. Por ejemplo, esto ocurre si intenta habilitar una región que está actualmente deshabilitada (en estado DESHABILITADO).

Código de estado HTTP: 409

## InternalServerErrorException

La operación falló debido a un error interno deAWS. Vuelva a intentar la operación más tarde.

Código de estado HTTP: 500

## TooManyRequestsException

La operación falló porque se realizó con demasiada frecuencia y superó el límite de aceleración.

Código de estado HTTP: 429

## ValidationException

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

Código de estado HTTP: 400

## Véase también

Para obtener más información sobre el uso de esta API en los SDK de AWS de un lenguaje específico, consulte:

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

- [AWSSDK para JavaScript V3](#)
- [SDK de AWS para PHP V3](#)
- [SDK de AWS para Python](#)
- [SDK de AWS para Ruby V3](#)

# GetAlternateContact

Recupera el contacto alternativo especificado adjunto a unCuenta de AWS.

Para obtener detalles completos sobre cómo utilizar las operaciones de contacto alternativas, consulte [Acceder a los contactos alternativos o actualizarlos](#).

## Note

Antes de poder actualizar la información de contacto alternativa de una Cuenta de AWS empresa gestionada porAWS Organizations, primero debe habilitar la integración entre AWS Account Management y Organizations. Para obtener más información, consulte [Habilitar el acceso confiable para la administración de AWS cuentas](#).

## 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 de la misma organización. La organización debe tener [todas las funciones habilitadas](#) y debe tener habilitado el [acceso de confianza](#) para el servicio de administración de cuentas y, si lo desea, debe tener asignada una cuenta de [administrador delegado](#).

 Note

La cuenta de administración no puede especificar la suya propia `AccountId`; debe llamar a la operación en un contexto independiente sin incluir el `AccountId` parámetro.

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 desee recuperar o modificar.

Tipo: String

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

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 produjo un error en la operación porque la identidad que realiza la llamada no tiene los permisos mínimos necesarios.

Código de estado HTTP: 403

### InternalServerError

La operación falló debido a un error interno de AWS. Vuelva a intentar la operación más tarde.

Código de estado HTTP: 500

### ResourceNotFoundException

La operación falló porque especificó un recurso que no se encuentra.

Código de estado HTTP: 404

## TooManyRequestsException

Se produjo un error en la operación porque se llamaba con demasiada frecuencia y se había superado el límite establecido.

Código de estado HTTP: 429

## ValidationException

La operación falló porque uno de los parámetros de entrada no era válido.

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 las 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 administración de cuentas.

### 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": "C00",
    "EmailAddress": "anika@example.com",
    "PhoneNumber": "206-555-0198"
  }
}
```

## Véase también

Para obtener más información sobre el uso de esta API en los SDK de AWS de un lenguaje específico, consulte:

- [Interfaz de la línea de comandos de AWS](#)
- [SDK de AWS para .NET](#)
- [SDK de AWS para C++](#)
- [SDK de AWS para Go](#)
- [SDK de AWS para Java V2](#)
- [AWSSDK para la versión 3 JavaScript](#)
- [SDK de AWS para PHP V3](#)

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

# GetContactInformation

Recupera la información de contacto principal de unCuenta de AWS.

Para obtener detalles completos sobre cómo utilizar las operaciones de contacto principal, consulte [Actualizar la información de contacto principal y alternativa](#).

## 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 el Cuenta de AWS 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 también debe ser una cuenta de miembro de la misma organización. La organización debe tener [todas las funciones habilitadas](#) y debe tener habilitado el [acceso de confianza](#) para el servicio de administración de cuentas y, si lo desea, debe tener asignada una cuenta de [administrador delegado](#).

#### Note

La cuenta de administración no puede especificar la suya propia. AccountId Debe llamar a la operación en un contexto independiente sin incluir el AccountId parámetro.

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

Tipo: String

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 unCuenta de AWS.

Tipo: objeto [ContactInformation](#)

## Errores

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

### AccessDeniedException

Se produjo un error en la operación porque la identidad que realiza la llamada no tiene los permisos mínimos necesarios.

Código de estado HTTP: 403

### InternalServerError

La operación falló debido a un error interno deAWS. Vuelva a intentar la operación más tarde.

Código de estado HTTP: 500

### ResourceNotFoundException

La operación falló porque especificó un recurso que no se encuentra.

Código de estado HTTP: 404

### TooManyRequestsException

Se produjo un error en la operación porque se llamaba con demasiada frecuencia y se había superado el límite establecido.

Código de estado HTTP: 429

### ValidationException

La operación falló porque uno de los parámetros de entrada no era válido.

Código de estado HTTP: 400

## Véase también

Para obtener más información sobre el uso de esta API en los SDK de AWS de un lenguaje específico, consulte:

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

# GetRegionOptStatus

Recupera el estado de suscripción de una región en particular.

## 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 el Cuenta de AWS 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 también debe ser una cuenta de miembro de la misma organización. La organización debe tener [todas las funciones habilitadas](#) y debe tener habilitado el [acceso de confianza](#) para el servicio de administración de cuentas y, si lo desea, debe tener asignada una cuenta de [administrador delegado](#).

#### Note

La cuenta de administración no puede especificar la suya propia. AccountId Debe llamar a la operación en un contexto independiente sin incluir el AccountId parámetro.

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

Tipo: String

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 ha transferido.

Tipo: cadena

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



## RegionOptStatus

Uno de los posibles estados que puede sufrir una región (Habilitada, Deshabilitada, Inhabilitada, Enabled\_By\_Default).

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 produjo un error en la operación porque la identidad que realiza la llamada no tiene los permisos mínimos necesarios.

Código de estado HTTP: 403

### InternalServerErrorException

La operación falló debido a un error interno deAWS. Vuelva a intentar la operación más tarde.

Código de estado HTTP: 500

### TooManyRequestsException

La operación falló porque se realizó con demasiada frecuencia y superó el límite de aceleración.

Código de estado HTTP: 429

### ValidationException

La operación falló porque uno de los parámetros de entrada no era válido.

Código de estado HTTP: 400

## Véase también

Para obtener más información sobre el uso de esta API en los SDK de AWS de un lenguaje específico, consulte:

- [Interfaz de la línea de comandos de AWS](#)
- [SDK de AWS para .NET](#)
- [SDK de AWS para C++](#)
- [SDK de AWS para Go](#)
- [SDK de AWS para Java V2](#)
- [AWSSDK para JavaScript V3](#)
- [SDK de AWS para PHP V3](#)
- [SDK de AWS para Python](#)
- [SDK de AWS 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 `region-opt-status-contains` parámetro.

### 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 el Cuenta de AWS 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 también debe ser una cuenta de miembro de la misma organización. La organización debe tener [todas las funciones habilitadas](#) y debe tener habilitado el [acceso de confianza](#) para el servicio de administración de cuentas y, si lo desea, debe tener asignada una cuenta de [administrador delegado](#).

#### Note

La cuenta de administración no puede especificar la suya propia. AccountId Debe llamar a la operación en un contexto independiente sin incluir el AccountId parámetro.

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

Tipo: String

Patrón: `^\d{12}$`

Obligatorio: no

### [MaxResults](#)

El número total de elementos que se van a devolver en el resultado del comando. Si el número total de elementos disponibles es superior al valor especificado, `NextToken` se proporciona a en el resultado 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 que se utiliza para especificar dónde empezar a paginar. Se trata `NextToken` de una respuesta previamente truncada. 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 los estados de las regiones (habilitada, deshabilitada, habilitada, 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 `ENABLING`, solo se mostrará una lista de regiones con el estado de `ENABLING` como región `ENABLING`.

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 `next-token` solicitud `delist-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 `filter` parámetro.

Tipo: Matriz de objetos [Region](#)

## Errores

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

### AccessDeniedException

Se produjo un error en la operación porque la identidad que realiza la llamada no tiene los permisos mínimos necesarios.

Código de estado HTTP: 403

### InternalServerErrorException

La operación falló debido a un error interno deAWS. Vuelva a intentar la operación más tarde.

Código de estado HTTP: 500

### TooManyRequestsException

La operación falló porque se realizó con demasiada frecuencia y superó el límite de aceleración.

Código de estado HTTP: 429

### ValidationException

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

Código de estado HTTP: 400

## Véase también

Para obtener más información sobre el uso de esta API en los SDK de AWS de un lenguaje específico, consulte:

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

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

# PutAlternateContact

Modifica el contacto alternativo especificado adjunto a unCuenta de AWS.

Para obtener detalles completos sobre cómo utilizar las operaciones de contacto alternativas, consulte [Acceder a los contactos alternativos o actualizarlos](#).

## Note

Antes de poder actualizar la información de contacto alternativa de una Cuenta de AWS empresa gestionada porAWS Organizations, primero debe habilitar la integración entre AWS Account Management y Organizations. Para obtener más información, consulte [Habilitar el acceso confiable para la administración de AWS cuentas](#).

## 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 de la misma organización. La organización debe tener [todas las funciones habilitadas](#) y debe tener habilitado el [acceso de confianza](#) para el servicio de administración de cuentas y, si lo desea, debe tener asignada una cuenta de [administrador delegado](#).

 Note

La cuenta de administración no puede especificar la suya propia `AccountId`; debe llamar a la operación en un contexto independiente sin incluir el `AccountId` parámetro.

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 desee recuperar o modificar.

Tipo: String

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. La longitud máxima es 64.

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 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.

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 produjo un error en la operación porque la identidad que realiza la llamada no tiene los permisos mínimos necesarios.

Código de estado HTTP: 403

### InternalServerErrorException

La operación falló debido a un error interno deAWS. Vuelva a intentar la operación más tarde.

Código de estado HTTP: 500

### TooManyRequestsException

La operación falló porque se realizó con demasiada frecuencia y superó el límite de aceleración.

Código de estado HTTP: 429

### ValidationException

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

Código de estado HTTP: 400

## Ejemplos

### Ejemplo 1

En el siguiente ejemplo, se establece el contacto alternativo de facturación de 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

El siguiente ejemplo establece o sobrescribe 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 administración de cuentas.

## 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 los SDK de AWS de un lenguaje específico, consulte:

- [Interfaz de la línea de comandos de AWS](#)
- [SDK de AWS para .NET](#)
- [SDK de AWS para C++](#)
- [SDK de AWS para Go](#)
- [SDK de AWS para Java V2](#)
- [AWSSDK para la versión 3 JavaScript](#)
- [SDK de AWS para PHP V3](#)
- [SDK de AWS para Python](#)
- [SDK de AWS para Ruby V3](#)

## PutContactInformation

Actualiza la información de contacto principal de unCuenta de AWS.

Para obtener detalles completos sobre cómo utilizar las operaciones de contacto principal, consulte [Actualizar la información de contacto principal y alternativa](#).

### 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 el

Cuenta de AWS 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 también debe ser una cuenta de miembro de la misma organización. La organización debe tener [todas las funciones habilitadas](#) y debe tener habilitado el [acceso de confianza](#) para el servicio de administración de cuentas y, si lo desea, debe tener asignada una cuenta de [administrador delegado](#).

 Note

La cuenta de administración no puede especificar la suya propia. AccountId Debe llamar a la operación en un contexto independiente sin incluir el AccountId parámetro.

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

Tipo: String

Patrón: `^\d{12}$`

Obligatorio: no

### [ContactInformation](#)

Contiene los detalles de la información de contacto principal asociada a unCuenta 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 produjo un error en la operación porque la identidad que realiza la llamada no tiene los permisos mínimos necesarios.

Código de estado HTTP: 403

### InternalServerErrorException

La operación falló debido a un error interno deAWS. Vuelva a intentar la operación más tarde.

Código de estado HTTP: 500

### TooManyRequestsException

La operación falló porque se realizó con demasiada frecuencia y superó el límite de aceleración.

Código de estado HTTP: 429

### ValidationException

La operación falló porque uno de los parámetros de entrada no era válido.

Código de estado HTTP: 400

## Véase también

Para obtener más información sobre el uso de esta API en los SDK de AWS de un lenguaje específico, consulte:

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



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

## Acciones relacionadas en otros AWS Servicios de

Las siguientes operaciones están relacionadas con AWS Account Management pero forman parte del AWS Organizations espacio de nombres:

- [CreateAccount](#)
- [Crear una cuenta de Gov Cloud](#)
- [DescribeAccount](#)

### CreateAccount

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

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

### Crear una cuenta de Gov Cloud

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

Para obtener más información, consulte [Crear una cuenta de Gov Cloud](#) en la AWS Organizations Referencia de la API.

### DescribeAccount

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

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

# Tipos de datos

Los tipos de datos siguientes son compatibles:

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

# AlternateContact

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

## Contenido

### AlternateContactType

El tipo de contacto alternativo.

Tipo: String

Valores válidos: BILLING | OPERATIONS | SECURITY

Obligatorio: no

### EmailAddress

La dirección de correo electrónico asociada a este contacto alternativo.

Tipo: String

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

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

Obligatorio: no

### Name

El nombre asociado a este contacto alternativo.

Tipo: String

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

Obligatorio: no

### PhoneNumber

El número de teléfono asociado a este contacto alternativo.

Tipo: String

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 25 caracteres.

Patrón: `^[\\s0-9()+-]+$`

Obligatorio: no

## Title

El título asociado a este contacto alternativo.

Tipo: String

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 un SDK de AWS de un lenguaje específico, consulte:

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

## ContactInformation

Contiene los detalles de la información de contacto principal asociada a unCuenta 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.

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 de país ISO-3166 de dos letras para la dirección de contacto principal.

Tipo: cadena

Restricciones de longitud: longitud fija de 2.

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 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 hay.

Tipo: cadena

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

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.

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: USCA, GBDE, 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 un SDK de AWS de un lenguaje específico, consulte:

- [SDK de AWS para C++](#)
- [AWS SDK para Go](#)
- [SDK de AWS 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 (Habilitado, Habilitado, Inhabilitado, Inhabilitado, Inhabilitado, Habilitado 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 un SDK de AWS de un lenguaje específico, consulte:

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

## ValidationExceptionField

La entrada no cumplió las restricciones especificadas por elAWS servicio en un campo especificado.

### Contenido

#### message

Un mensaje sobre la excepción de validación.

Tipo: String

Obligatorio: sí

#### name

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

Tipo: String

Obligatorio: sí

### Véase también

Para obtener más información sobre el uso de esta API en un SDK de AWS de un lenguaje específico, consulte:

- [AWS SDK para C++](#)
- [AWS SDK para Go](#)
- [AWS SDK para Java V2](#)
- [SDK de AWS 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 deAWS API](#) en la Guía del usuario de IAM.

## Action

Las acciones que se van a realizar.

Tipo: cadena

Obligatorio: sí

## Version

La versión de la API para la que está escrita la solicitud, expresada en el formato AAAA-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 deAWS 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 valor válido de X-Amz-Date para 20120325T120000Z.

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

Tipo: string

Obligatorio: condicional

### X-Amz-Security-Token

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

Condición: si utiliza credenciales de seguridad temporales deAWS STS, debe incluir el token de seguridad.

Tipo: string

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 deAWS 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 servicios de AWS. 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 solicitud no se ajusta a los estándares de AWS.

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 certificado X.509 o el ID de clave de acceso de AWS proporcionado no existen en nuestros registros.

Código de estado HTTP: 403

#### NotAuthorized

No tiene permiso para realizar esta acción.

Código de estado HTTP: 400

#### OptInRequired

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

Código de estado HTTP: 403

#### RequestExpired

La solicitud llegó al servicio más de 15 minutos después de la marca de fecha en la solicitud o más de 15 minutos después de la fecha de vencimiento de la solicitud (por ejemplo, para las URL prefirmadas) o la marca de fecha de la solicitud corresponde a una hora futura en más de 15 minutos.

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 se denegó debido a una limitación controlada.

Código de estado HTTP: 400

#### ValidationError

La entrada no satisface las limitaciones que especifica un servicio de AWS.

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 paraAWSAdministración de 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 hacer llamadas directas alAWSAPI de consultas de administración de cuentas, puede utilizar una de lasAWS SDK. El SDK de AWS consta de bibliotecas y código de muestra para diversos lenguajes de programación y plataformas (Java, Ruby, .NET, iOS, Android, etc.). Los SDK proporcionan una forma cómoda de crear un acceso programático aAWSAdministración de cuentas yAWS. Por ejemplo, los SDK se encargan de tareas como firmar solicitudes criptográficamente, gestionar los errores y reintentar las solicitudes de forma automática. Para obtener información sobre los SDK de AWS (por ejemplo, cómo descargarlos e instalarlos), consulte [Herramientas para Amazon Web Services](#).

Con la API de consulta paraAWSAdministración de cuentas, puede llamar a acciones de servicio. Las solicitudes de API de consulta son solicitudes de HTTPS que deben contener unActionparámetro para indicar la operación que se va a realizar.AWS Soportes de administración de cuentasGETyPOSTsolicitudes para todas las operaciones. Es decir, la API no requiere que utilicesGETpara algunas acciones yPOSTpara otros. Sin embargo,GETlas solicitudes están sujetas al tamaño limitado de una URL. Aunque este límite depende del navegador, el límite típico es de 2048 bytes. Por lo tanto, para las solicitudes de la API de consulta que requieren tamaños más grandes, debe utilizar unPOSTsolicitud.

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](#)
- [FirmandoAWSSolicitudes de API de administración de cuentas](#)

## Puntos de conexión

AWSAccount Management tiene un único punto final de API global que se aloja en el este de EE. UU. (Virginia del Norte)Región de AWS.

Para obtener más información sobreAWSpuntos de conexión y regiones para todos los servicios, consulte[Regiones y puntos finales](#)en elReferencia general de AWS.

## HTTPS obligatorio

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

## FirmandoAWSSolicitudes de API de administración de cuentas

Las solicitudes deben firmarse con un ID de clave de acceso y una clave de acceso secreta. Le recomendamos encarecidamente que no utilice suAWScredenciales de cuenta raíz para el trabajo diario conAWSAdministración de cuentas. Puede utilizar las credenciales paraAWS Identity and Access Managementcredenciales de usuario o temporales (IAM), como las que se utilizan con un rol de IAM.

Para firmar las solicitudes de la API, debe utilizar Signature Version 4 de AWS. Para obtener información sobre Signature Version 4, consulte [Firma de solicitudes API de AWS](#) en la Guía del usuario de IAM.

Para obtener más información, consulte lo siguiente:

- [Credenciales de seguridad de AWS](#): ofrece información general acerca de los tipos de credenciales que puede utilizar para acceder a AWS.
- [Mejores prácticas de seguridad en IAM](#)— Ofrece sugerencias para usar el servicio IAM para ayudar a proteger suAWSrecursos, incluidos los deAWSAdministración de cuentas.
- [Credenciales temporales de seguridad en IAM](#): describe cómo crear y utilizar las credenciales temporales de seguridad.



## Cuotas para AWS Account Management

Su Cuenta de AWS tiene cuotas predeterminadas, anteriormente conocidas como “límites”, para cada servicio de AWS. 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 de contactos alternativos en una Cuenta de AWS	3: uno para cada uno BILLINGSECURITY, y OPERATIONS
Número de solicitudes de suscripción regional simultáneas por cuenta	6
Número de solicitudes simultáneas de suscripción regional por organización	20
Tasa de solicitudes por cuenta DeleteAlternateContact	1 por segundo, ráfaga a 6 por segundo
Tasa de DisableRegion solicitudes por cuenta	1 por segundo, ráfaga a 1 por segundo
Tasa de EnableRegion solicitudes por cuenta	1 por segundo, ráfaga a 1 por segundo
Tasa de GetAlternateContact solicitudes por cuenta	10 por segundo, ráfaga a 15 por segundo
Tasa de GetContactInformation solicitudes por cuenta	10 por segundo, ráfaga a 15 por segundo
Tasa de GetRegionOptStatus solicitudes por cuenta	5 por segundo, ráfaga a 5 por segundo
Tasa de ListRegions solicitudes por cuenta	5 por segundo, ráfaga a 5 por segundo

Recurso	Cuota
Tasa de PutAlternateContact solicitudes por cuenta	5 por segundo, ráfaga a 8 por segundo
Tasa de PutContactInformation solicitudes por cuenta	5 por segundo, ráfaga a 8 por segundo

# Solución de problemas de su Cuenta de AWS

Utilice la información de los siguientes temas como ayuda para diagnosticar y solucionar problemas con su Cuenta de AWS. Para obtener ayuda con el usuario root, consulte [Solución de problemas con el usuario root](#) en la Guía del usuario de IAM. Para obtener ayuda con el proceso de inicio de sesión, consulte [Solución de problemas de inicio de Cuenta de AWS sesión en la Guía del usuario](#) de inicio de AWSsesión.

## Temas de solución de problemas

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

## Solución de problemas con Cuenta de AWS la creación

Utilice la información que aquí se incluye para solucionar problemas relacionados para crear una Cuenta de AWS. Si tienes problemas para iniciar sesión en tu nueva cuenta después de haberla creado, consulta [Solución de problemas de inicio de Cuenta de AWS sesión en la Guía](#) de inicio de AWSsesión.

### Problemas

- [No he recibido la llamada de AWS para verificar mi cuenta nueva](#)
- [Cuando intento verificarlo mi Cuenta de AWS por teléfono, aparece un error sobre el "número máximo de intentos fallidos"](#)
- [Han pasado más de 24 horas y mi cuenta no está activada](#)

## No he recibido la llamada de AWS para verificar mi cuenta nueva

Al crear una Cuenta de AWS, debes proporcionar un número de teléfono en el que puedas recibir un mensaje SMS o una llamada de voz. Debe especificar qué método utilizar para verificar el número.


Si no recibe el mensaje o la llamada, compruebe lo siguiente:

- Que ingresó el número de teléfono correcto y seleccionó el código de país correcto durante el proceso de registro.

- Si utilizas un teléfono móvil, asegúrate de tener una señal móvil para recibir mensajes SMS o llamadas.
- La información que haya introducido para el [método de pago](#) es correcta.

Si no recibiste un SMS o una llamada para completar el proceso de verificación de identidad, AWS Support podemos ayudarte a activarlo Cuenta de AWS manualmente. Utilice los siguientes pasos:

1. Asegúrese de que lo puedan contactar al [número de teléfono](#) que proporcionó para su Cuenta de AWS.
2. Abra la [AWS Supportconsola](#) y elija Crear caso.
  - a. Elija Soporte de cuentas y facturación
  - b. En Tipo, seleccione Cuenta.
  - c. En Categoría, seleccione Activación.
  - d. En la sección de Descripción del caso, indique la fecha y la hora en las que podamos contactarlo.
  - e. En la sección Opciones de contacto, seleccione Chat para ver los Métodos de contacto.
  - f. Elija Enviar.

 Note

Puedes crear un caso AWS Support incluso si aún Cuenta de AWS no lo has activado.

Cuando intento verificarlo mi Cuenta de AWS por teléfono, aparece un error sobre el "número máximo de intentos fallidos"

AWS Support puede ayudarlo a activar su cuenta manualmente. Siga estos pasos:

1. [Inicie sesión en su Cuenta de AWS](#) con la dirección de correo electrónico y la contraseña que especificó al crear su cuenta.
2. Abra la [consola AWS Support](#) y elija Crear caso.
3. Elija Soporte de cuentas y facturación
4. En Tipo, seleccione Cuenta.
5. En Categoría, seleccione Activación.

6. En la sección de Descripción del caso, indique la fecha y la hora en las que podamos contactarlo.
7. En la sección Opciones de contacto, seleccione Chat para ver los Métodos de contacto.
8. Elija Enviar.

AWS Support lo contactará y intentará activar manualmente su Cuenta de AWS.

## Han pasado más de 24 horas y mi cuenta no está activada

En ocasiones, la activación de la cuenta puede retrasarse. Si el proceso tarda más de 24 horas, compruebe lo siguiente:

- Finalice el proceso de activación de la cuenta.

Si ha cerrado la ventana del proceso de registro antes de añadir toda la información necesaria, abra la página de [registro](#). Seleccione Iniciar sesión en una cuenta existente Cuenta de AWS e inicie sesión con la dirección de correo electrónico y la contraseña que eligió para la cuenta.

- Compruebe la información asociada a su método de pago.

En la consola AWS Billing and Cost Management, consulte los [Métodos de pago](#) para ver si hay errores.

- Póngase en contacto con su institución financiera.

En ocasiones, las instituciones financieras rechazan las solicitudes de autorización de AWS. Póngase en contacto con la institución asociada a su método de pago y pídale que apruebe las solicitudes de autorización de AWS. AWS cancela la solicitud de autorización tan pronto como la apruebe su institución financiera, por lo que no se le cobrará por la solicitud de autorización. Es posible que las solicitudes de autorización sigan figurando como un pequeño cargo (normalmente 1 USD) en los estados de cuenta de su institución financiera.

- Revise su correo electrónico y su carpeta de correo no deseado para ver si hay solicitudes de información adicional.
- Pruebe con otro navegador.
- Póngase en contacto con AWS Support.

Póngase en contacto con [AWS Support](#) para obtener ayuda. Mencione cualquier paso de solución de problemas que ya haya probado.

**Note**

No proporcione información confidencial, como números de tarjetas de crédito, en ninguna correspondencia con AWS.

## Solución de problemas relacionados con Cuenta de AWS el cierre

Usa la información que aparece a continuación para ayudarte a diagnosticar y solucionar los problemas habituales que se producen 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 cuentas](#)
- [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» al intentar cerrar la cuenta de un miembro](#)
- [¿Debo eliminar mi AWS organización antes de cerrar la cuenta de administración?](#)

### No sé cómo eliminar o cancelar mi cuenta

Para cerrar tu cuenta, sigue las instrucciones que se indican en [Cerrar un Cuenta de AWS](#).

### No veo el botón Cerrar cuenta en la página de cuentas

Si no ha iniciado sesión como usuario root, no verá el botón Cerrar cuenta en la página de cuentas. Debe [iniciar sesión AWS Management Console como usuario root](#) para cerrar su cuenta. Si no puedes iniciar sesión, consulta [Solución de problemas con el usuario root](#).

### 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 Cuenta de AWS. Si no recibes este correo electrónico [en unas horas, puedes iniciar sesión](#)

[AWS Management Console como usuario root](#) para comprobar que tu cuenta está cerrada. Si tu cuenta se ha cerrado correctamente, aparecerá un mensaje que indica que tu cuenta está cerrada. Si la cuenta que has cerrado es una cuenta de miembro, puedes comprobar si el cierre se ha realizado correctamente comprobando si la cuenta cerrada está etiquetada como SUSPENDED 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 miembros activas. Solo puedes cerrar la cuenta de administración si tu 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 Suspended junto a sus nombres de cuenta. Después, 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 AWS Management Console como usuario raíz de la](#) cuenta de administración y cerrarla desde la página de cuentas. Para obtener más información, consulte [Cerrar una cuenta de administración en su organización](#) en la Guía del AWS Organizations usuario.

## Recibo el mensaje de error «CLOSE\_ACCOUNT\_QUOTA\_EXCEEDED» al intentar cerrar la cuenta de un 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 de una cuenta es de 10 y el cierre máximo es de 1000, incluso si el 10% de las cuentas supera las 1000. Para obtener más información sobre las cuotas de Organizations, consulte [Cuotas for AWS Organizations](#) en la Guía del AWS Organizations usuario.

## ¿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 puedes cerrar la cuenta de administración si tu 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 Suspended junto a sus nombres de cuenta. Después, puede cerrar la cuenta de administración.

## Solución de problemas con Cuentas de AWS

Utilice la información que se indica aquí para solucionar problemas relacionados con Cuenta de AWS.

### Problemas

- [Quiero cambiar la tarjeta de crédito de Cuenta de AWS](#)
- [Quiero informar fraudulenta Cuenta de AWS actividad](#)
- [Quiero cerrar mi Cuenta de AWS](#)

## Quiero cambiar la tarjeta de crédito de Cuenta de AWS

Para cambiar la tarjeta de crédito de Cuenta de AWS, debe poder iniciar la sesión. AWS dispone de protecciones que requieren que demuestre que es el propietario de la cuenta de. Para obtener instrucciones, consulte [Administración de los métodos de pago con tarjeta de crédito](#) en la AWS Billing Guía del usuario de.

## Quiero informar fraudulenta Cuenta de AWS actividad

Si sospechas que hay actividad fraudulenta utilizando tu Cuenta de AWS y quisiera hacer un informe, véase [¿Por dónde informar sobre abuso de AWS recursos?](#)

Si tienes problemas con una compra realizada en Amazon.com, consulte [Servicio al cliente de Amazon](#).

## Quiero cerrar mi Cuenta de AWS

Para obtener ayuda para solucionar problemas con el cierre de Cuenta de AWS, consulte [Cerrar un Cuenta de AWS](#).



# Historial de documentos de la Guía del usuario de administración de cuentas

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

Cambio	Descripción	Fecha
<a href="#">Reescritura del tema del cierre de cuentas</a>	Revisó por completo todo el tema del cierre de cuentas, incluyendo la adición de pasos sobre cómo cerrar cuentas de miembros y cuentas de administración.	1 de febrero de 2024
<a href="#">Fin del soporte para añadir nuevas preguntas sobre desafíos de seguridad</a>	Se ha añadido un nuevo contenido, en el que se indica que la opción de añadir nuevas preguntas de desafío se ha eliminado de la página de cuentas.	5 de enero de 2024
<a href="#">Fin del soporte para el aws-portal espacio de nombres</a>	AWS Identity and Access Management(IAM) las acciones que antes se utilizaban para administrar tu cuenta (por ejemplo, <code>aws-portal:ModifyAccount</code> y <code>aws-portal:ViewAccount</code> ) han llegado al final del soporte estándar.	1 de enero de 2024
<a href="#">Reescribe el tema de las regiones</a>	Se revisó por completo todo el tema de las regiones, incluida la adición de controles de expansión y contracción.	8 de octubre de 2023

<a href="#">Se reubicaron los temas para los usuarios raíz en la Guía del usuario de IAM</a>	Se consolidó el debate sobre los usuarios raíz en un tema y se agregaron enlaces de referencia cruzada a los temas de los usuarios raíz que se trasladaron a la Guía del usuario de IAM.	18 de septiembre de 2023
<a href="#">Se agregó una nueva sección al tema de contacto de la cuenta principal</a>	Se agregó una nueva sección de requisitos de número de teléfono y dirección de correo electrónico.	12 de septiembre de 2023
<a href="#">Nuevas API de información de contacto</a>	Support para nuevas <code>GetContactInformation</code> <code>PutContactInformation</code> API.	22 de julio de 2022
<a href="#">AWS La administración de cuentas ahora permite actualizar contactos alternativos a través de la AWS Organizations consola.</a>	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
<a href="#">Versión inicial</a>	Versión inicial de la guía de referencia sobre la administración de AWS cuentas	30 de septiembre de 2021

# Glosario de AWS

Para ver la terminología más reciente de AWS, consulte el [Glosario de AWS](#) en la Referencia de Glosario de AWS.

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.