AWS Organizations

Guía del usuario

AWS Organizations: Guía del usuario

Table of Contents

¿Qué es AWS Organizations?

AWS Organizationses unaccount (p. 6)que le permite consolidar múltiples Cuentas de AWS en unorganizaciónque cree y administre de forma centralizada.AWS Organizationsincluye capacidades de administración de cuentas y facturación unificada que le permiten satisfacer mejor las necesidades presupuestarias, de seguridad y de conformidad de su empresa. Como administrador de su organización, puede crear cuentas e invitar a cuentas existentes a unirse a la organización.

Esta guía de usuario define conceptos clave para AWS Organizations, proporciona tutoriales y explica cómo crear y administrar una organización.

Temas

- Características de AWS Organizations (p. 1)
- Precios de AWS Organizations (p. 3)
- Acceso a AWS Organizations (p. 3)
- Soporte y comentarios de AWS Organizations (p. 4)

Características de AWS Organizations

AWS Organizations ofrece las siguientes características:

Administración centralizada de todos los Cuentas de AWS

Puede combinar sus cuentas existentes en una organización para poder administrar las cuentas de forma centralizada. Puede crear cuentas que se conviertan automáticamente en parte de su organización y puede invitar a otras cuentas a que se unan a su organización. También puede asociar políticas que afecten a algunas o a todas sus cuentas.

Facturación unificada para todas las cuentas miembro

La facturación unificada es una característica de AWS Organizations. Puede utilizar la cuenta de administración de la organización para consolidar y pagar por todas las cuentas miembro. En la facturación unificada, las cuentas de administración también pueden tener acceso a la información de facturación, la información de la cuenta y la actividad de la cuenta de las cuentas miembro de su organización. Esta información se puede utilizar para servicios como Cost Explorer, que puede ayudar a las cuentas de administración a mejorar el rendimiento de los costos de su organización.

Agrupar jerárquicamente todas sus cuentas para satisfacer sus necesidades presupuestarias, de seguridad y de conformidad

Puede agrupar sus cuentas en unidades organizativas y asociar diferentes políticas de acceso a cada una de ellas. Por ejemplo, si tiene cuentas que deben tener acceso solo a los servicios de AWS que cumplan determinados requisitos normativos, puede incluirlas en una unidad organizativa. A continuación, puede asociar una política a esa unidad organizativa que bloquee el acceso a los servicios que no cumplan los requisitos normativos. Puede anidar unidades organizativas en otras unidades organizativas, hasta un máximo de cinco niveles de profundidad, lo que proporciona flexibilidad en el modo de estructurar sus grupos de cuentas.

Políticas para centralizar el control sobre laAWSLos servicios y las acciones de API a las que puede tener acceso cada cuenta

Como administrador de la cuenta de administración de una organización, puede utilizar políticas de control de servicios (SCP) para especificar los permisos máximos de las cuentas miembro de la

organización. En las SCP, puede restringir a qué servicios, recursos y acciones de API individuales de AWS pueden obtener acceso los usuarios y roles de cada cuenta de miembro. También puede definir condiciones respecto a cuándo restringir el acceso a los servicios, los recursos y las acciones de la API de AWS. Estas restricciones se aplican incluso a los administradores de las cuentas miembro de la organización. Cuando AWS Organizations bloquea el acceso a una acción de la API, un recurso o un servicio en una cuenta de miembro, un usuario o rol de dicha cuenta no puede acceder a ella. Este bloqueo permanece en vigor aunque un administrador de una cuenta miembro conceda dichos permisos de forma explícita en una política de IAM.

Para obtener más información, consulte Políticas de control de servicios (p. 108).

Políticas para estandarizar las etiquetas en los recursos de las cuentas de su organización

Puede utilizar políticas de etiquetas para mantener la coherencia de las etiquetas, incluido el tratamiento de casos preferentes de valores y claves de etiquetas.

Para obtener más información, consulte Políticas de etiquetas (p. 195)

Políticas para controlar cómoAWSla inteligencia artificial (IA) y los servicios de aprendizaje automático pueden recopilar y almacenar datos.

Puede utilizar las políticas de exclusión de los servicios de IA para optar por no participar en la recopilación y el almacenamiento de datos para cualquiera de losAWSLos servicios de IA que no desea utilizar.

Para obtener más información, consulte Políticas de exclusión de servicios de IA (p. 144)

Políticas que configuran copias de seguridad automáticas de los recursos de las cuentas de su organización

Puede usar directivas de copia de seguridad para configurar y aplicar automáticamenteAWS Backupplanea recursos en todas las cuentas de su organización.

Para obtener más información, consulte Políticas de copia de seguridad (p. 160)

Integración y compatibilidad conAWS Identity and Access Management(IAM)

IAMproporciona un control detallado sobre los usuarios y roles de las distintas cuentas.AWS Organizationsamplía ese control al nivel de cuenta al permitirle controlar lo que los usuarios y roles de una cuenta o grupo de cuentas pueden hacer. Los permisos resultantes son la intersección lógica de lo que permiteAWS OrganizationsEn el nivel de cuenta y los permisos que concede explícitamente IAM en el nivel de usuario o de función dentro de esa cuenta. En otras palabras, el usuario solo puede tener acceso a lo que permiteAmboselAWS Organizationspolíticas y políticas de IAM. Si alguna bloquea una operación, el usuario no puede tener acceso a esa operación.

Integración con otrosAWSservices

Puede aprovechar los servicios de administración de varias cuentas de AWS Organizations con servicios seleccionados de AWS para realizar tareas en todas las cuentas que son miembros de su organización. Para obtener una lista de los servicios y los beneficios de utilizar cada servicio en la organización, consulte Servicios de AWS que se pueden utilizar con AWS Organizations (p. 237).

Cuando habilita unaAWSPara realizar tareas en su nombre en las cuentas miembro de su organización,AWS Organizationscrea unFunción vinculada al servicio de IAMPara ese servicio en cada cuenta miembro. El rol vinculado al servicio tiene permisos de IAM predefinidos que permiten que los otrosAWSPara realizar tareas específicas en la organización y las cuentas de esta. Para que esto funcione, todas las cuentas de una organización disponen automáticamente de un rol vinculado a servicios. Este rol habilita elAWS OrganizationsPara crear los roles vinculados al servicio necesarios porAWSpara los que habilita el acceso de confianza. Estos roles vinculados a servicios adicionales están asociados a políticas de permisos de IAM que permiten que el servicio especificado lleve a cabo únicamente las tareas necesarias según sus opciones de configuración. Para obtener más información, consulte Uso de AWS Organizations con otros servicios de AWS. (p. 232).

Acceso global

AWS Organizationses un servicio global con un único punto de enlace que funciona desde cualquier Regiones de AWS . No es necesario seleccionar explícitamente una región en la que operar.

Replicación de datos que tienen consistencia final

Al igual que muchos otros servicios de AWS, AWS Organizations proporciona una consistencia final. AWS Organizations ofrece una alta disponibilidad, ya que replica datos entre varios servidores ubicados en centros de datos de AWS de su región. Si una solicitud para cambiar algunos datos se realiza correctamente, el cambio se confirma y se almacena de forma segura. Sin embargo, el cambio se debe replicar en varios servidores. Para obtener más información, consulte Los cambios que realizo no están siempre visibles inmediatamente (p. 337).

Uso gratuito

AWS Organizationses una característica de la Cuenta de AWS se ofrece sin cargo adicional. Solo se le cobrará cuando acceda a otrosAWSLos servicios de las cuentas de de su organización. Para obtener información acerca de los precios de otrosAWS, consulte laPágina de precios de Amazon Web Services.

Precios de AWS Organizations

AWS Organizations se ofrece sin cargo adicional. Solo se le cobrarán los recursos de AWS que usen los usuarios y las funciones de las cuentas miembro. Por ejemplo, se le cobrará la tarifa estándar de las instancias de Amazon EC2 que utilicen los usuarios o roles de las cuentas miembro. Para obtener información acerca de los precios de otrosAWSservicios, consulteAWSPrecios.

Acceso a AWS Organizations

Puede trabajar con AWS Organizations de cualquiera de las siguientes formas:

AWS Management Console

La consola de AWS Organizations es una interfaz basada en navegador que puede utilizar para administrar su organización y sus recursos de AWS. Puede llevar a cabo cualquier tarea en su organización utilizando la consola.

AWS Herramientas de línea de comandos

Mediante las herramientas de la línea de comandos de AWS, puede emitir comandos en la línea de comandos de su sistema para realizar tareas de AWS Organizations y AWS. El uso de la línea de comandos puede ser más rápido y cómo que utilizar la consola. Las herramientas de línea de comandos también son útiles para crear scripts que realicen tareas de AWS.

AWS proporciona dos conjuntos de herramientas de línea de comandos:

- AWS Command Line Interface(AWS CLI). Para obtener información acerca del modo de instalar y usar laAWS CLI, consulte laAWS Command Line InterfaceGuía del usuario.
- AWS Tools for Windows PowerShell. Para obtener información acerca del modo de instalar y usar las herramientas para Windows PowerShell, consulte laAWS Tools for Windows PowerShellGuía del usuario.

AWS SDK

Los SDK de AWS se componen de bibliotecas y código de muestra para diversos lenguajes de programación y plataformas (por ejemplo, Java, Python, Ruby, .NET, iOS y Android). Los SDK se

encargan de tareas como firmar solicitudes criptográficamente, gestionar los errores y reintentar las solicitudes de forma automática. Para obtener más información acerca de los SDK de AWS, incluido cómo descargarlos e instalarlos, consulte Herramientas para Amazon Web Services.

AWS Organizations API de consulta HTTPS de

La API de consulta HTTPS de AWS Organizations le ofrece acceso mediante programación a AWS Organizations y AWS. La API de consulta HTTPS le permite emitir solicitudes HTTPS directamente al servicio. Cuando use la API HTTPS, debe incluir código para firmar digitalmente las solicitudes utilizando sus credenciales. Para obtener más información, consulteLlamar a la API mediante solicitudes de consulta HTTPy laAWS OrganizationsReferencia de la API.

Soporte y comentarios de AWS Organizations

Agradecemos sus comentarios. Puede enviar sus comentarios afeedback-awsorganizations@amazon.com. También puede publicar sus comentarios y preguntas en nuestro foro de soporte deAWS Organizations. Para obtener más información acerca de los foros de soporte de AWS, consulte la Ayuda de los foros.

Otros recursos de AWS

- AWSCapacitación y cursos de formación técnica: enlaces a cursos basados en roles y especializados, y también a laboratorios autoguiados para ayudarle a desarrollar suAWShabilidades y adquirir experiencia práctica.
- AWSHerramientas para desarrolladores: enlaces a herramientas y recursos para desarrolladores que proporcionan documentación, ejemplos de código, notas de la versión y otra información para ayudarle a crear aplicaciones innovadoras conAWS.
- AWS SupportCenter: el centro para crear y administrar suAWSCasos de Support. También incluye enlaces a otros recursos útiles como foros, preguntas técnicas frecuentes, estado de los servicios y AWS Trusted Advisor.
- AWSSoporte: página web principal con información acerca deAWSSupport, un canal de soporte individualizado y de respuesta rápida para ayudarle a crear y ejecutar aplicaciones en la nube.
- ContactoUn punto central de contacto para las consultas relacionadas conAWSFacturación, cuentas, eventos, abuso y otros problemas de.
- AWSTérminos del sitio: información detallada sobre nuestros derechos de autor y marca comercial, su cuenta, licencia y acceso al sitio, entre otros temas.

Introducción a AWS Organizations

Los siguientes temas le ayudarán a aprender acerca de AWS Organizations y cómo utilizarlo.

Más información sobre...

Terminología y conceptos de AWS Organizations (p. 5)

Conozca la terminología y los conceptos básicos necesarios para entender AWS Organizations. Esta sección describe cada uno de los componentes de una organización y los aspectos básicos sobre cómo trabajan conjuntamente para ofrecer un nuevo nivel de control sobre lo que pueden hacer los usuarios en dichas cuentas.

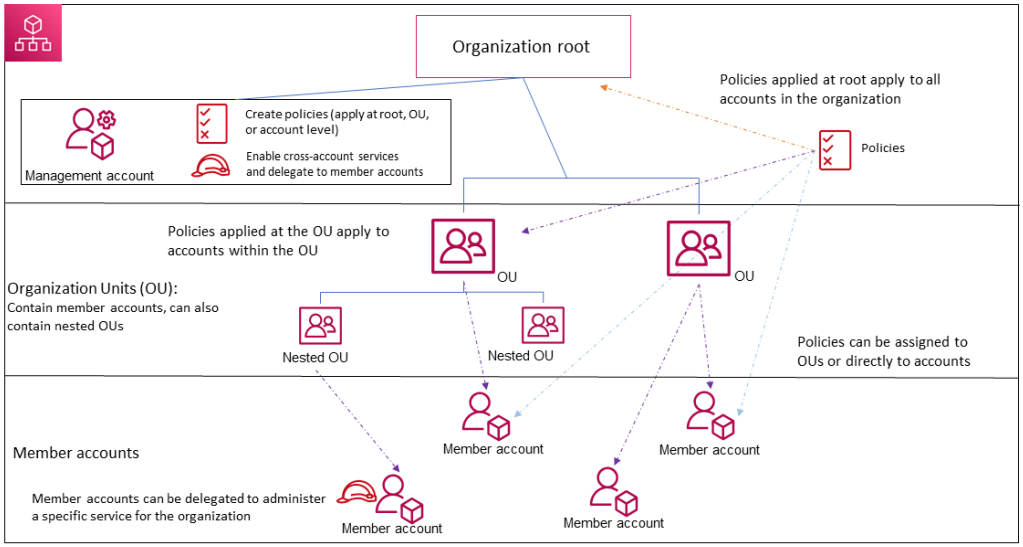
Facturación unificada para organizaciones

Una de las características principales de AWS Organizations es la consolidación de la facturación de todas las cuentas de la organización. Obtenga más información acerca de cómo se gestiona la facturación en una organización y cómo funcionan los distintos descuentos funcionando cuando se comparten entre varias cuentas. This content is in the AWS Billing and Cost Management User Guide.

Terminología y conceptos de AWS Organizations

En este tema se explican algunos de los conceptos clave que debe conocer para comenzar a utilizar AWS Organizations.

En el siguiente diagrama se muestra una organización básica que se compone de cinco cuentas organizadas en cuatro unidades organizativas bajo el directorio raíz. La organización también dispone de varias políticas asociadas a algunas de las unidades organizativas o directamente a las cuentas. Para obtener una descripción de cada uno de estos elementos, consulte las definiciones incluidas en este tema.



Organization

Una entidad que crea para consolidar suAWS cuentas (p. 6)De esta forma, puede administrarlos como una única unidad. Puede utilizar la consola de AWS Organizations para ver y administrar de forma centralizada todas las cuentas de su organización. Una organización tiene una cuenta de administración junto con cero o más cuentas miembro. Puede organizar las cuentas jerárquicamente en una estructura de árbol con un nodo raíz (p. 6) en la parte superior y unidades organizativas (p. 6) anidadas bajo el nodo raíz. Cada cuenta puede estar directamente en el nodo raíz o colocarse en una de las unidades organizativas de la jerarquía. Una organización tiene la funcionalidad determinada por el conjunto de características (p. 7) habilitadas.

Nodo raíz

El contenedor principal de todas las cuentas de su organización. Si aplica una política al nodo raíz, esta se aplica a todas las unidades organizativas (p. 6) y cuentas (p. 6) de la organización.

> Note
>
> En la actualidad, puede disponer de un solo nodo raíz, que AWS Organizations crea automáticamente cuando usted crea su organización.

Unidad organizativa

Un contenedor para las cuentas (p. 6) de un nodo raíz (p. 6). Una unidad organizativa también puede contener otras unidades organizativas, lo que le permite crear una jerarquía que se asemeja a un árbol invertido, con un nodo raíz en la parte superior y ramas de unidades organizativas descendentes que terminan en las cuentas (las hojas del árbol). Cuando asocia una política a uno de los nodos de la jerarquía, esta se transmite y aplica a todas las ramas (unidades organizativas) y hojas (cuentas) que se encuentran debajo. Una unidad organizativa puede tener uno y solo un nodo raíz y cada cuenta puede ser miembro de exactamente una unidad organizativa.

Cuenta

Una cuenta en Organizations es un estándar Cuenta de AWS que contiene suAWSrecursos y las identidades que pueden acceder a esos recursos.

> Tip
>
> Un registroAWScuenta esnolo mismo que una «cuenta de usuario». Un registroAWSusuario dees una identidad que crea usandoAWS Identity and Access Management(IAM) y toma la forma de unUsuario de IAM con credenciales a largo plazo, o unRol de IAM con credenciales a corto plazo. Un soloAWSpuede, y normalmente contiene muchos usuarios y roles.

Hay dos tipos de cuentas en una organización: una cuenta única que se denomina la cuenta de administración y una o más cuentas miembro.

- LaCuenta de administraciónes la cuenta que usa para crear la organización. Desde la cuenta de administración de la organización, puede hacer lo siguiente:
  - Crear cuentas en la organización
  - Invitar a otras cuentas existentes a la organización
  - Eliminar cuentas de la organización
  - Administrar invitaciones
  - Aplicar políticas a entidades (nodos raíz, unidades organizativas o cuentas) dentro de la organización
  - Habilite la integración conAWSpara proporcionar funcionalidad de servicio en todas las cuentas de la organización.

  La cuenta de gestión tiene las responsabilidades de unCuenta del pagadory es responsable de pagar todos los cargos generados por las cuentas miembro. No puede cambiar la cuenta de administración de una organización.

- Cuentas de miembroscomponen todas las cuentas del resto de cuentas de una organización. Una cuenta no puede pertenecer a más de una organización a la vez. Puede asociar una política a una cuenta para aplicar controles a esa sola cuenta.

Invitación

El proceso de pedir a otra cuenta (p. 6) que se una a su organización (p. 6). Únicamente la cuenta de administración de la organización puede emitir una invitación. La invitación se amplía al ID de la cuenta o a la dirección de correo electrónico asociada a la cuenta invitada. Una vez que la cuenta invitada acepta una invitación, pasa a ser una cuenta miembro de la organización. También se pueden enviar invitaciones a todas las cuentas miembro actuales cuando la organización necesita que todos los miembros aprueben el cambio de admitir únicamente las características de la facturación unificada (p. 7) a admitir todas las características (p. 7) de la organización. Las invitaciones funcionan mediante el intercambio de protocolos de enlace (handshakes) (p. 7) entre cuentas. Es posible que no vea protocolos de enlace cuando trabaja en la consola de AWS Organizations. No obstante, si utiliza la AWS CLI o la API de AWS Organizations, tiene que trabajar directamente con los protocolos de enlace.

Protocolo de enlace

Un proceso de varios pasos para intercambiar información entre dos partes. Uno de sus usos principales en AWS Organizations es servir de implementación subyacente de las invitaciones (p. 7). Los mensajes de protocolos de enlace se transfieren entre el iniciador del protocolo de enlace y el destinatario y los responden ellos mismos. Los mensajes se transfieren de una forma que ayuda a garantizar que ambas partes sepan cuál es el estado actual. Los protocolos de enlace se usan también cuando la organización cambia de admitir solo las características de facturación unificada (p. 7) a admitir todas las características (p. 7) que ofrece AWS Organizations. Por lo general, solo necesita interactuar con los protocolos de enlace si trabaja en la API o en las herramientas de línea de comandos de AWS Organizations, como la AWS CLI.

Conjuntos de características disponibles

- Todas las características: el conjunto de características predeterminadas disponibles enAWS Organizations. Incluye toda la funcionalidad de facturación unificada, además de características avanzadas que le ofrecen mayor control sobre las cuentas de su organización. Por ejemplo, cuando todas las características están habilitadas, la cuenta de administración de la organización tiene control completo sobre lo que las cuentas miembro pueden hacer. La cuenta de administración puede aplicarSCP (p. 108)Para restringir los servicios y las acciones a los que los usuarios (incluido el usuario raíz) y roles de una cuenta tienen acceso. La cuenta de administración también puede evitar que las cuentas miembro abandonen la organización.También puede habilitar la integración con soporteAWSPara permitir que esos servicios proporcionen funcionalidad en todas las cuentas de su organización.

  Puede crear una organización con todas las características ya habilitadas, o puede habilitar todas las características en una organización que originalmente solo admitía las características de facturación unificada. Para habilitar todas las características, todas las cuentas miembro invitadas deben aprobar el cambio aceptando la invitación que se envía cuando la cuenta de administración inicia el proceso.

- facturación unificada— Este conjunto de funciones proporciona funcionalidad de facturación compartida, peronoincluyen las características más avanzadas deAWS Organizations. Por ejemplo, no puede habilitar otrasAWSservicios para integrarse con su organización para trabajar en todas sus cuentas,o use políticas para restringir lo que los usuarios y los roles de diferentes cuentas pueden hacer. Para utilizar las características avanzadas de AWS Organizations, debe habilitar todas las características (p. 7) de la organización.

Política de control de servicios (SCP)

Una política que especifica los servicios y las acciones que los usuarios y roles pueden utilizar en las cuentas afectadas por la SCP (p. 108). Las SCP son similares a las políticas de permisos de IAM, con la salvedad de que no conceden permisos. En lugar de ello, las SCP especifican el máximo de

permisos para una organización, unidad organizativa (OU) o cuenta. Al asociar una SCP al nodo raíz de la organización o a una unidad organizativa, la SCP limita los permisos para las entidades de las cuentas de miembros.

Listas de permitidos frente a listas de denegación

Las listas de permitidos y las listas de denegación son estrategias complementarias para cuando se aplican políticas SCP (p. 108) para filtrar los permisos que están disponibles para las cuentas.

- Permitir la estrategia de lista: especifique de forma explícita el acceso queespermitido. Cualquier otro acceso estará bloqueado implícitamente. De forma predeterminada, AWS Organizations asocia una política administrada de AWS llamada `FullAWSAccess` a todos los nodos raíz, las unidades organizativas y las cuentas. Esto ayuda a garantizar que, a medida que crea su organización, nada se bloquee hasta que usted quiera bloquearlo. Es decir, de forma predeterminada, todos los permisos están habilitados. Cuando esté listo para restringir los permisos, sustituya la política `FullAWSAccess` por una que permita únicamente el conjunto de permisos más limitados que desee. Los usuarios y roles de las cuentas afectadas solo tendrán ese nivel de acceso, aunque las políticas de IAM les permitan todas las acciones. Si reemplaza la política predeterminada en el nodo raíz, las restricciones afectarán a todas las cuentas de la organización. No puede volver a agregar permisos posteriormente en un nivel inferior de la jerarquía porque una SCP nunca concede permisos; solo los filtra.
- Estrategia de listas: especifique de forma explícita el acceso queno espermitido. El resto del acceso estará permitido. En este caso, todos los permisos están permitidos a menos que se bloqueen de forma explícita. Este es el comportamiento predeterminado de AWS Organizations. De forma predeterminada, AWS Organizations asocia una política administrada de AWS llamada `FullAWSAccess` a todos los nodos raíz, las unidades organizativas y las cuentas. Esto permite a cualquier cuenta tener acceso a cualquier servicio u operación sin restricciones impuestas por AWS Organizations. A diferencia de la técnica de lista de permitidos que se ha descrito anteriormente, cuando utiliza las listas de denegación, se suele dejar la política de `FullAWSAccess` predeterminada en vigor (que permite "todos"). No obstante, luego debe asociar políticas adicionales que denieguen explícitamente el acceso a las acciones y los servicios no deseados. De la misma forma que con las políticas de permisos IAM, una denegación explícita de una acción del servicio invalida cualquier permiso para esa acción.

Política de exclusión de servicios de inteligencia artificial (IA)

Un tipo de directiva que le ayuda a estandarizar la configuración de exclusión paraAWSServicios de IA en todas las cuentas de su organización. CiertosAWSLos servicios de IA pueden almacenar y utilizar el contenido del cliente procesado por dichos servicios para el desarrollo y la mejora continua de los servicios y tecnologías de IA de Amazon. Como unAWScliente, puede usarPolíticas de exclusión de servicios de IA (p. 144)para optar por no tener su contenido almacenado o utilizado para mejoras de servicio.

Política Backup

Un tipo de política que le ayuda a estandarizar e implementar una estrategia de copia de seguridad de los recursos de todas las cuentas de su organización. En unPolítica de copia (p. 160), puede configurar e implementar planes de copia de seguridad para sus recursos.

Política de etiquetas

Un tipo de política que le ayuda a estandarizar las etiquetas de todos los recursos de todas las cuentas de su organización. En una política de etiquetas (p. 195), puede especificar las reglas de etiquetado de recursos específicos.

Tutoriales de AWS Organizations

Utilice los tutoriales de esta sección para aprender a realizar tareas con AWS Organizations.

Tutorial: Creación y configuración de una organización (p. 9)

Comience con instrucciones paso a paso para crear su organización, invitar a sus primeras cuentas miembro crear una jerarquía de unidades organizativas que contenga las cuentas y aplicar algunas políticas de control de servicios (SCP).

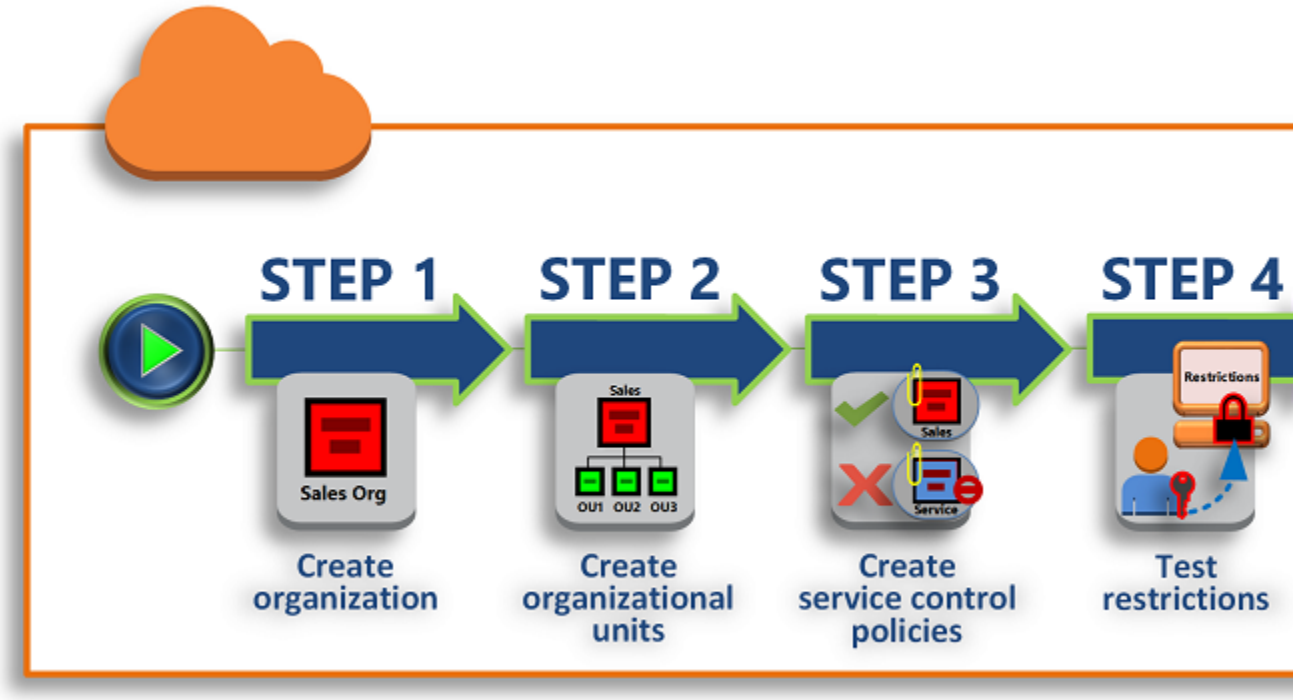
Tutorial: Monitoreo de cambios importantes en la organización con CloudWatch Events (p. 18)

Para monitorear los cambios clave de su organización, puede configurar de modo que active una «alarma» (un correo electrónico, un mensaje de texto SMS o una entrada de registro) cuando en su organización se produzcan las acciones que haya designado. Por ejemplo, muchas organizaciones desean saber cuándo se crea una cuenta nueva o cuándo una cuenta intenta salir de la organización.

Tutorial: Creación y configuración de una organización

En este tutorial, creará su organización y la configurará con dos cuentas miembro de AWS. Creará una de las cuentas miembro en su organización e invitará a la otra cuenta a que se una a su organización. A continuación, utilice elLista de permitidos (p. 8)Para especificar que los administradores de cuentas pueden delegar únicamente los servicios y las acciones que se indican explícitamente. Esto permite a los administradores validar cualquier nuevo servicio que AWS introduce antes de permitir que lo use cualquier otra persona de la empresa. De esta forma, si AWS introduce un nuevo servicio, este sigue estando prohibido hasta que un administrador lo añada a la lista de permitidos de la política correspondiente. En este tutorial también se muestra cómo utilizar una políticaLista de denegación (p. 8)Para asegurarse de que ningún usuario de una cuenta miembro pueda cambiar la configuración de los registros de auditoría queAWS CloudTrailCreate.

En la siguiente ilustración se muestran los principales pasos del tutorial.



Paso 1: Crear la organización (p. 11)

En este paso, crea una organización con el nodo de Cuenta de AWS como cuenta de gestión. También invitas a uno Cuenta de AWS Para unirse a la organización y crea una segunda cuenta como cuenta miembro.

Paso 2: Crear las unidades organizativas (p. 13)

A continuación, crea dos unidades organizativas en la nueva organización e incluye las cuentas miembro en esas unidades organizativas.

Paso 3: Crear las políticas de control de servicios (p. 14)

Las políticas de control de servicios (SCP) (p. 108) sirven para aplicar restricciones a las acciones que se pueden delegar en los usuarios y roles de las cuentas miembro. En este paso, crea dos políticas SCP y las asocia a las unidades organizativas de su organización.

Paso 4: Probar las políticas de su organización (p. 18)

Puede iniciar sesión como un usuario de cada una de las cuentas de prueba y ver los efectos que las SCP tienen en las cuentas.

Ninguno de los pasos de este tutorial supondrá un costo en su factura de AWS. AWS Organizations es un servicio gratuito.

Prerequisites

En este tutorial, se supone que tiene acceso a dos de las Cuentas de AWS (creará una tercera como parte de este tutorial) y que puede iniciar sesión en cada una de ellas como administrador.

El tutorial hace referencia a las cuentas de la manera siguiente:

- `111111111111`: la cuenta que usa para crear la organización. Esta cuenta pasa a ser la cuenta de administración. El propietario de esta cuenta tiene una dirección de correo electrónico de `OrgAccount111@example.com`.
- `222222222222`: una cuenta que invita a unirse a la organización como cuenta miembro. El propietario de esta cuenta tiene una dirección de correo electrónico de `member222@example.com`.
- `333333333333`: una cuenta que crea como miembro de la organización. El propietario de esta cuenta tiene una dirección de correo electrónico de `member333@example.com`.

Sustituya los valores anteriores por los valores asociados con las cuentas de prueba. Le recomendamos que no utilice cuentas de producción para este tutorial.

Paso 1: Crear la organización

En este paso, inicia sesión en la cuenta 111111111111 como administrador, crea una organización con esa cuenta como cuenta de administración y, a continuación, invita a una cuenta existente, 2222222222, a unirse como cuenta miembro.

AWS Management Console

1. Inicie sesión enAWScomo administrador de la cuenta 111111111111 y abra la.AWS Organizationsconsole.
2. En la página de introducción, elijaCrear una organización.
3. En el cuadro de diálogo de confirmación, elijaCrear una organización.

   Note

   De forma predeterminada, la organización se crea con todas las características habilitadas. También puede crear la organización únicamente con las características de facturación unificada (p. 7) habilitadas.

   AWScrea la organización y le muestra el Cuentas de AWS (Se ha creado el certificado). Si estás en una página diferente, elige Cuentas de AWS En el panel de navegación de la izquierda.

   Si la cuenta que usas nunca ha tenido su dirección de correo electrónico verificada porAWSSe envía automáticamente un correo electrónico de verificación a la dirección asociada a la cuenta de administración. Puede pasar algún tiempo hasta que reciba el correo electrónico de verificación.
4. Verifique la dirección de correo electrónico en un plazo de 24 horas. Para obtener más información, consulte Verificación de dirección de correo electrónico (p. 36).

Ahora tiene una organización con su cuenta como único miembro. Esta es la cuenta de administración de la organización.

Invitar a una cuenta existente a que se una a su organización

Ahora que tiene una organización, puede comenzar a rellenarla con cuentas. En los pasos de esta sección, invita a una cuenta existente a unirse como miembro de su organización.

AWS Management Console

Para invitar a una cuenta existente a unirse

1. Vaya a la . Cuentas de AWS y elijaAdición de un Cuenta de AWS .
2. En la páginaAdición de un Cuenta de AWS elija, elijaInvite a un Cuenta de AWS .

3. En el cuadroDirección de correo electrónico o ID de cuenta de un Cuenta de AWS InvitarEn, escriba la dirección de correo electrónico del propietario de la cuenta a la que desea invitar, similar a la siguiente: **`member222@example.com`**. Alternativamente, si conoce la Cuenta de AWS Número de identificación, entonces puede ingresarlo en su lugar.
4. Escriba el texto que desee en el cuadro de textoMensaje que incluir en el mensaje de correo electrónico de invitación. Este texto se incluirá en el correo electrónico que se envía al propietario de la cuenta.
5. SeleccionarEnviar invitación.AWS Organizationsenvía la invitación al propietario de la cuenta.

   Important

   Si obtiene un error que indica que ha excedido los límites de la cuenta para la organización o que no puede añadir una cuenta porque la organización sigue inicializándose, espere a que pase una hora desde que creó la organización e inténtelo de nuevo. Si el error persiste, póngase en contacto con AWSSupport.
6. A efectos de este tutorial, ahora tiene que aceptar su propia invitación. Realice alguna de las siguientes acciones para ir a la página Invitations en la consola:

   - Abra el correo electrónico queAWSDesde la cuenta de gestión y elija el enlace para aceptar la invitación. Cuando se le pida que inicie sesión, hágalo como administrador de la cuenta miembro invitada.
   - Abra el iconoAWS Organizationsconsoley vaya a la.Invitaciones(Se ha creado el certificado).
7. En la página Cuentas de AWS elija, elijaAceptarHaga clic en y luego enConfirmar.
8. Cerrar la sesión de la cuenta miembro e inicie sesión de nuevo como administrador en la cuenta de administración.

Crear una cuenta miembro

En los pasos de esta sección, crea un nodo de Cuenta de AWS que es automáticamente miembro de la organización. En este tutorial nos referimos a esta cuenta como 3333333333.

AWS Management Console

Para crear una cuenta miembro

1. En la páginaAWS OrganizationsConsola de, en el Cuentas de AWS elija, elijaAdd Cuenta de AWS .
2. En la páginaAdición de un Cuenta de AWS elija, elijaCreación de un Cuenta de AWS .
3. Para Cuenta de AWS Nombre de, escriba un nombre para la cuenta, como**`MainApp Account`**.
4. ParaDirección de correo electrónico del usuario raíz de la cuentaEn, escriba la dirección de correo electrónico de la persona que va a recibir las comunicaciones en nombre de la cuenta. Este valor debe ser único de forma global. Dos cuentas no pueden tener la misma dirección de correo electrónico. Por ejemplo, puede escribir un correo como **`mainapp@example.com`**.
5. En IAM role name, puede dejar este campo en blanco para que se use automáticamente el nombre de rol predeterminado de `OrganizationAccountAccessRole` o puede proporcionar su propio nombre. Esta función le permite tener acceso a la nueva cuenta miembro cuando inicie sesión como un usuario de IAM en la cuenta de administración. En este tutorial, déjelo en blanco para indicar a AWS Organizations que va a crear la función con el nombre predeterminado.
6. Seleccione Create Cuenta de AWS . Es posible que tenga que esperar un rato y actualizar la página para ver la nueva cuenta en Cuentas de AWS (Se ha creado el certificado).

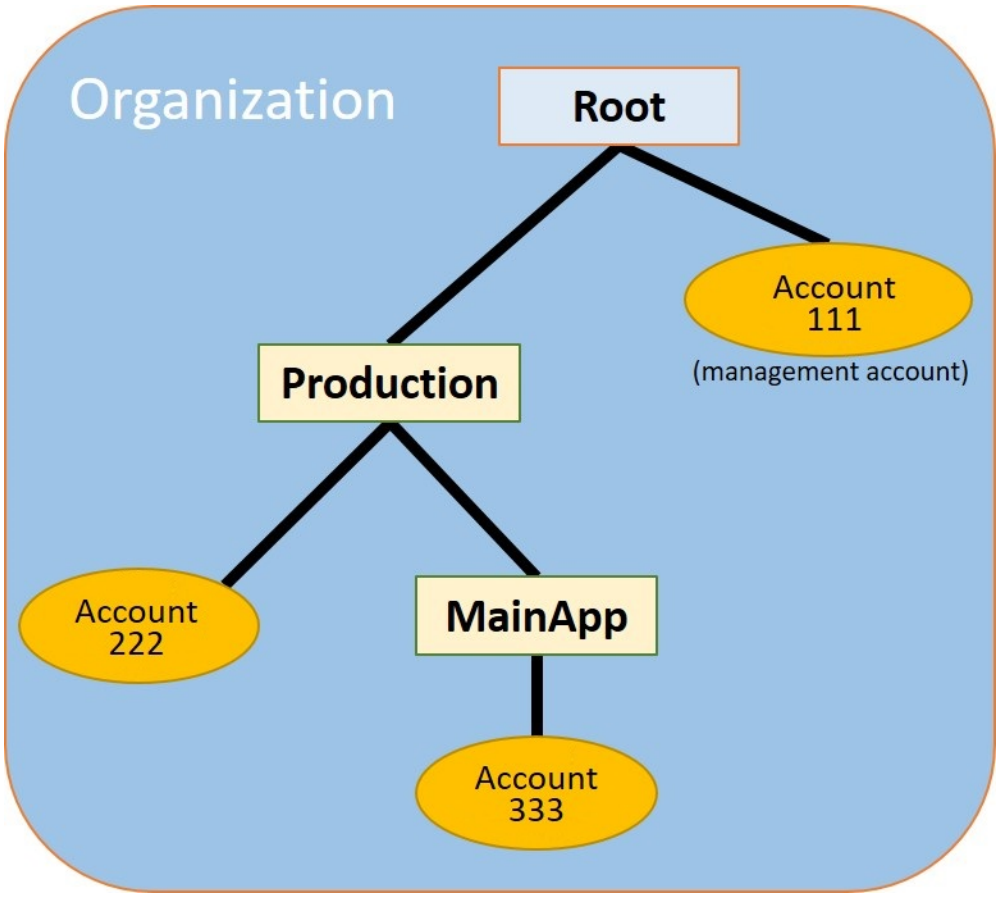
   Important

   Si obtiene un error que indica que ha excedido los límites de la cuenta para la organización o que no puede añadir una cuenta porque la organización sigue

inicializándose, espere a que pase una hora desde que creó la organización e inténtelo de nuevo. Si el error persiste, póngase en contacto con AWSSupport.

Paso 2: Crear las unidades organizativas

En los pasos de esta sección, crea unidades organizativas e incluye en ellas sus cuentas miembro. Cuando termine, su jerarquía tendrá un aspecto similar al de la siguiente ilustración. La cuenta de administración permanece en el nodo raíz. Una cuenta miembro se mueve a la unidad organizativa Production y la otra cuenta miembro se mueve a la unidad organizativa MainApp, que es una unidad organizativa secundaria de Production.



AWS Management Console

Para crear y rellenar las unidades organizativas

Note

En los pasos siguientes, interactúa con objetos para los que puede elegir el nombre del objeto en sí o el botón de opción situado junto al objeto.

- Si elige el nombre del objeto, abra una nueva página que muestre los detalles de los objetos.
- Si elige el botón de opción situado junto al objeto, está identificando ese objeto para actuar mediante otra acción, como elegir una opción de menú.

Los pasos que siguen le permiten elegir el botón de opción para que pueda actuar sobre el objeto asociado mediante la elección del menú.

1. En la páginaAWS OrganizationsconsoleVaya a la. Cuentas de AWS (Se ha creado el certificado).
2. Asegúrese de que el conmutadorVista Cuentas de AWS Soloestá giradoDESACER .
3. Active la casillajunto a laRootContenedor.
4. En la páginaLos niñoselija, elijaActionsy, a continuación, enunidad organizativa, elijaCrear nuevos.
5. En la páginaCrear unidad organizativa en Raíz, para elNombre de la unidad organizativa, introduzca**`Production`**Haga clic en y luego enCrear unidad organizativa.
6. Active la casillajunto a su nuevoProducciónOU.
7. SeleccionarActionsy, a continuación, enunidad organizativa, elijaCrear nuevos.
8. En la páginaCrear unidad organizativa en ProducciónPara el nombre de la segunda unidad organizativa, escriba**`MainApp`**Haga clic en y luego enCrear unidad organizativa.

   Ahora puede mover sus cuentas miembro a estas unidades organizativas.
9. Vuelva a la. Cuentas de AWS y, a continuación, expanda el árbol debajo de suProducciónOU eligiendo el triángulojunto a él.

   Esto muestra elMainAppOU como hijo deProducción.
10. Active la casilla, no su nombre), elijaActionsy, a continuación, en Cuenta de AWS , elijaMover.
11. En la páginaMover Cuenta de AWS '***`nombre-cuenta-miembro`***', elija el botón de opción, no su nombre) y luego elijaMover Cuenta de AWS .
12. Active la casilla, no su nombre), elijaActionsy, a continuación, en Cuenta de AWS , elijaMover.
13. En la páginaMover Cuenta de AWS '***`nombre-cuenta-miembro`***', el triángulo situado junto aProducciónpara expandir esa rama y exponerMainApp.
14. Elija el botón de opción, no su nombre) y luego bajo Cuenta de AWS , elijaMover Cuenta de AWS .

Paso 3: Crear las políticas de control de servicios

En los pasos de esta sección, crearemos tres políticas de control de servicios (SCP) (p. 108) y las asocia al nodo raíz y a las unidades organizativas para restringir lo que los usuarios de cuentas de la organización pueden hacer. La primera SCP impide que cualquiera de las cuentas miembro cree o modifique los registros de AWS CloudTrail que haya configurado. La cuenta de administración no se ve afectada por ninguna SCP; por lo tanto, debe crear los registros desde dicha cuenta después de aplicar CloudTrail SCP de.

Activar el tipo de política de control de servicios para la organización

Antes de asociar una política de algún tipo a una raíz o unidad organizativa dentro de una raíz, debe habilitar el tipo de política para la organización. De forma predeterminada, los tipos de políticas no están habilitados. Los pasos de esta sección le indican cómo habilitar el tipo de política de control de servicios (SCP) para su organización.

AWS Management Console

Para habilitar las SCP para la organización

1. Vaya a la .Políticasy, a continuación, elijaPolíticas de control de servicios.
2. En la páginaPolíticas de control de servicioselija, elijaActivar políticas de control de servicios.

   Aparece un banner verde para informarle de que ahora puede crear SCPs en su organización.

Cree sus SCP

Ahora que las directivas de control de servicios están habilitadas en su organización, puede crear las tres directivas que necesita para este tutorial.

AWS Management Console

Para crear el primer SCP que bloquea acciones de configuración de CloudTrail

1. Vaya a la .Políticasy, a continuación, elijaPolíticas de control de servicios.
2. En la página Service control policies (Políticas de control de servicios), seleccione Create policy (Crear política).

   Note

   El editor de políticas de control de servicios está disponible actualmente en la versión original deAWS Organizationsconsola de . Cuando complete las ediciones, volverá automáticamente a la nueva versión de la consola.
3. Para Policy name (Nombre de política), introduzca **`Block CloudTrail Configuration Actions`**.
4. En el navegadorPolítica deEn la lista de servicios de la izquierda, seleccione CloudTrail para el servicio. A continuación, elija una de las siguientes acciones: AddTags,CreateTrail,DeleteTrail,RemoveTags,StartLogging,StopLogging, yUpdateTrail.
5. En el panel de la izquierda, elijaAdd resource (Añadir recurso)y especifiqueCloudTrailyTodos los recursos. A continuación, elija Add resource (Añadir recurso).

   La instrucción de la política de la derecha se actualizará y tendrá un aspecto similar al siguiente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1234567890123",
            "Effect": "Deny",
            "Action": [
                "cloudtrail:AddTags",
                "cloudtrail:CreateTrail",
                "cloudtrail:DeleteTrail",
                "cloudtrail:RemoveTags",
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging",
                "cloudtrail:UpdateTrail"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

6. Elija Create Policy (Crear política).

La segunda política define una lista de permitidos (p. 8) de todos los servicios y acciones que desea permitir para los usuarios y roles de la unidad organizativa Production. Cuando haya finalizado, los usuarios de la unidad organizativa Production (Producción) podrán obtener acceso solo a los servicios y acciones enumerados.

AWS Management Console

Para crear la segunda política que permite usar los servicios aprobados para la unidad organizativa de producción

1. Desde elPolíticas de control de servicioselija, elijaCrear política.
2. Para Policy name (Nombre de política), introduzca **`Allow List for All Approved Services`**.
3. Sitúe el cursor en el panel derecho de la sección Policy (Política) y pegue una política como la siguiente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1111111111111",
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "elasticloadbalancing:*",
                "codecommit:*",
                "cloudtrail:*",
                "codedeploy:*"
              ],
            "Resource": [ "*" ]
        }
    ]
}
```

4. Elija Create Policy (Crear política).

La política final proporciona una lista de denegación (p. 8) de servicios que están bloqueados en la unidad organizativa MainApp. En este tutorial, bloquea el acceso a Amazon DynamoDB en cualquier cuenta que esté enMainAppOU.

AWS Management Console

Para crear la tercera política que deniega el acceso los servicios que no se pueden utilizar en la unidad organizativa MainApp

1. Desde elPolíticas de control de servicioselija, elijaCrear política.
2. Para Policy name (Nombre de política), introduzca **`Deny List for MainApp Prohibited Services`**.
3. En el navegadorPolítica de, a la izquierda, seleccioneAmazon DynamoDBpara el servicio. Para la acción, elija All actions (Todas las acciones).
4. En el panel de la izquierda, elijaAdd resource (Añadir recurso)y especifiqueDynamoDByTodos los recursos. A continuación, elija Add resource (Añadir recurso).

   La instrucción de la política de la derecha se actualizará y tendrá un aspecto similar al siguiente.

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

5. Elija Create policy para guardar la SCP.

Asociar las políticas SCP a sus unidades organizativas

Ahora que las SCP están disponibles y habilitadas para su nodo raíz, puede asociarlas al nodo raíz y a las unidades organizativas.

AWS Management Console

Para asociar las políticas al nodo raíz y a las unidades organizativas

1. Vaya a la página Cuentas de AWS .
2. En la página Cuentas de AWS elija, elijaRoot(su nombre, no el botón de opción) para navegar a su página de detalles.
3. En la páginaRoot, elija la página de detalles dePolíticasy, a continuación, enPolíticas de control de servicios, elijaAttach.
4. En la páginaAdjuntar una política de control de servicios, elija el botón de opción que hay junto al SCP denominado`Block CloudTrail Configuration Actions`Haga clic en y luego enAttach. En este tutorial, la asocia al módulo raíz para que afecte a todas las cuentas miembro para impedir que alguien modifique la forma en que ha configurado CloudTrail.

   LaRootpágina de detalles,Políticasmuestra ahora que hay dos políticas SCP asociadas a la raíz: la que acaba de asociar y la política predeterminada`FullAWSAccess`SCP
5. Vuelva a la. Cuentas de AWS y elija laProducciónOU (es el nombre, no el botón de opción) para navegar a su página de detalles.
6. En la páginaProducciónPágina de detalles de la unidad organizativa, elija la.Políticas.
7. EnPolíticas de control de servicios, elijaAttach.
8. En la páginaAdjuntar una política de control de servicios, elija el botón de opción que hay junto a`Allow List for All Approved Services`Haga clic en y luego enAttach. Esto permite a los usuarios o roles en las cuentas de miembro en elProducciónOU para acceder a los servicios aprobados.
9. Elija el iconoPolíticasPara ver que hay dos SCP asociadas a la OU: la que acaba de asociar y la`FullAWSAccess`SCP Sin embargo, debido a que el`FullAWSAccess`SCP también permite todos los servicios y acciones, debe desasociar esta política para asegurarse de que solo se permitan los servicios aprobados.
10. Para eliminar la política predeterminada de la.ProducciónOU, elija el botón de opción paraFullAWSAccess, elijaSepararY, a continuación, en el cuadro de diálogo de confirmación, elijaPolítica de desvinculación.

    Después de quitar esta directiva predeterminada, todas las cuentas de miembro de laProducciónOU pierde inmediatamente el acceso a todas las acciones y servicios que no estén en la política SCP de lista de permitidos que se ha asociado en los pasos anteriores. Cualquier

solicitud para utilizar acciones que no estén incluidas en la SCP Allow List for All Approved Services (Lista de permitidos para todos los servicios aprobados) se deniega. Esto es así incluso si un administrador de una cuenta concede acceso a otro servicio asociando una política de permisos de IAM a un usuario de una de las cuentas miembro.

11. Ahora puede adjuntar la política SCP denominada `Deny List for MainApp Prohibited services` para impedir que algún usuario de las cuentas de la unidad organizativa MainApp use alguno de los servicios restringidos.

    Para ello, vaya a la. Cuentas de AWS , elija el icono del triángulo para expandir elProducciónOU y, a continuación, elija laMainAppOU (su nombre, no el botón de opción) para desplazarse hasta su contenido.
12. En la páginaMainApp, elija la página de detalles dePolíticas.
13. EnPolíticas de control de serviciosEn la lista de políticas disponibles, elija el botón de opción situado junto aDenegar la lista de servicios prohibidos por MainAppHaga clic en y luego enAsociar política.

Paso 4: Probar las políticas de su organización

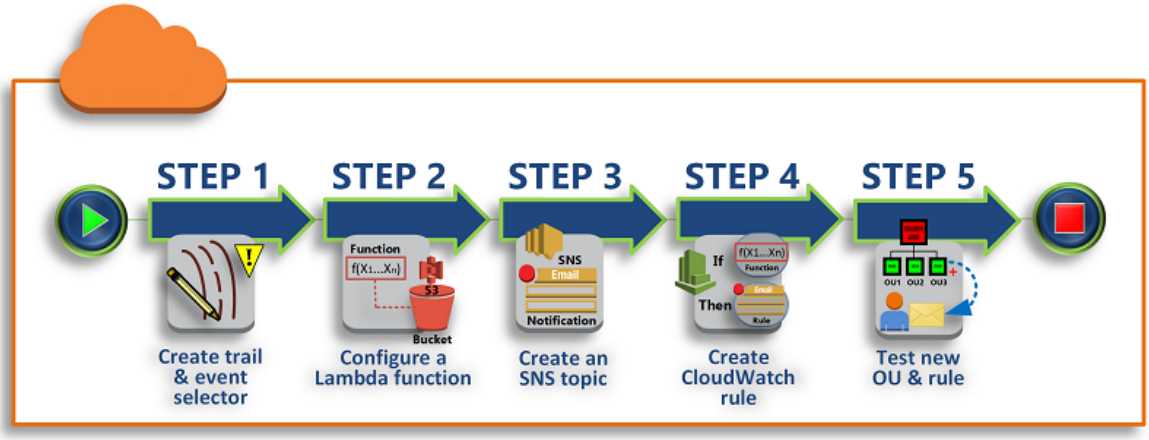
Ahora puede iniciar sesión como un usuario de cualquiera de las cuentas miembro e intentar realizar algunas acciones de AWAWS:

- Si inicia sesión como un usuario de la cuenta de administración, puede realizar cualquier operación permitida por las políticas de permisos de IAM. Los SCP no afectan a ningún usuario o rol de la cuenta de administración, independientemente de en qué unidad organizativa o unidad organizativa se encuentre la cuenta.
- Si inicia sesión como usuario raíz o como un usuario de IAM en la cuenta 2222222222, puede realizar cualquier acción permitida por la lista de permitidos.AWS Organizationsdeniega cualquier intento de realizar una acción en algún servicio que no esté en la lista de permitidos. Además,AWS Organizationsdeniega cualquier intento de realizar alguna de las acciones de configuración de CloudTrail.
- Si inicia sesión como un usuario de la cuenta 3333333333, puede realizar cualquier acción permitida por la lista de permitidos y no bloqueada por la lista de denegación.AWS Organizationsdeniega cualquier intento de realizar una acción que no esté en la política de lista de permitidos y cualquier acción que esté en la política de lista de denegación. Además,AWS Organizationsdeniega cualquier intento de realizar alguna de las acciones de configuración de CloudTrail.

Tutorial: Monitoreo de cambios importantes en la organización con CloudWatch Events

En este tutorial se muestra cómo configurar los cambios en su organización. Para comenzar, se configura una regla que se activa cuando los usuarios invocan determinadas operaciones de AWS Organizations. A continuación, configura CloudWatch Events para ejecutar unAWS LambdaCuando se active la regla y se configura Amazon SNS para que envíe un correo electrónico con información detallada sobre el evento.

En la siguiente ilustración se muestran los principales pasos del tutorial.



Paso 1: Configuración de un selector de seguimiento y de eventos (p. 20)

Cree un registro de seguimiento en AWS CloudTrail. Configúrelo para capturar todas las llamadas a API.

Paso 2: Configuración de una función Lambda (p. 21)

Cree una función AWS Lambda que registre los detalles del evento en un bucket de S3.

Paso 3: Cree un tema de Amazon SNS que envía correos electrónicos a los suscriptores (p. 21)

Cree un tema de Amazon SNS que envíe correos electrónicos a sus suscriptores y, a continuación, suscríbase a ese tema.

Paso 4: Crear una regla de eventos de CloudWatch (p. 22)

Cree una regla que indique a los eventos de CloudWatch que pase determinados datos de las llamadas a API especificadas a la función Lambda y a los suscriptores al tema de SNS.

Paso 5: Prueba de la regla de CloudWatch Events (p. 23)

Ejecute una de las operaciones monitorizadas para probar la nueva regla. En este tutorial, la operación monitorizada crea una unidad organizativa (OU). Puede ver la entrada de registro creada por la función Lambda y el correo electrónico que Amazon SNS envía a los suscriptores.

Tip

También puede utilizar este tutorial como guía al configurar operaciones similares como, por ejemplo, el envío de notificaciones por correo electrónico cuando se haya completado la creación de la cuenta. Dado que la creación de la cuenta es una operación asíncrona, no recibirá de forma predeterminada una notificación cuando se complete. Para obtener más información sobre el uso deAWS CloudTraily CloudWatch Events conAWS Organizations, consulteRegistro y monitoreo en AWS Organizations (p. 321).

Prerequisites

Este tutorial se basa en los siguientes supuestos:

- Puede iniciar sesión en laAWS Management Consolecomo usuario de IAM de la cuenta de administración de su organización. El usuario de IAM debe tener permisos para crear y configurar un registro en CloudTrail, una función en Lambda, un tema en Amazon SNS y una regla en CloudWatch.

Para obtener más información sobre la concesión de permisos, consulteAdministración de accesosen laGuía del usuario de IAMo la guía del servicio para el que desea configurar el acceso.

- Dispone de acceso a un bucket de Amazon Simple Storage Service (Amazon S3) (o tiene permisos para crear un bucket) con el fin de recibir el registro de CloudTrail que ha configurado en el paso 1.

> **Important**
>
> En la actualidad,AWS OrganizationsSe aloja únicamente en la región de EE.UU. Este (Norte de Virginia) (aunque está disponible en todo el mundo). Para realizar los pasos de este tutorial, debe configurar la AWS Management Console para que utilice esa región.

Paso 1: Configuración de un selector de seguimiento y de eventos

En este paso, iniciará sesión en la cuenta de administración y configurará un registro deRegistro de seguimiento de) enAWS CloudTrail. Además, configurará un selector de eventos en el registro de seguimiento para capturar todas las llamadas a API de lectura/escritura, de tal forma que existan llamadas que permitan que CloudWatch se active.

Para crear un registro de seguimiento

1. Inicie sesión enAWSA continuación, abra la consola de CloudTrail enhttps://console.aws.amazon.com/cloudtrail/.
2. En la barra de navegación de la esquina superior derecha de la consola, elija la opciónEE.UU. Este (Norte de Virginia)Región . Si eliges una región diferente,AWS OrganizationsNo aparecerá entre las opciones de la configuración de CloudWatch Events y CloudTrail no capturará la información sobreAWS Organizations.
3. En el panel de navegación, seleccione Trails.
4. Elija Create Trail (Crear registro de seguimiento).
5. En Trail name (Nombre del registro de seguimiento), escriba **`My-Test-Trail`**.
6. Realice una de las siguientes opciones para especificar dónde debe entregarse los registros de CloudTrail:
   - Si ya tiene un bucket, elija No junto a Create a new S3 bucket (Crear un nuevo bucket de S3) y, a continuación, elija el nombre del bucket en la lista S3 bucket (Bucket de S3).
   - Si necesita crear un bucket, elija Yes (Sí) junto a Create a new S3 bucket (Crear un nuevo bucket de S3) y, a continuación, escriba el nombre del nuevo bucket en S3 bucket (Bucket de S3).

     > **Note**
     >
     > Los nombres de los buckets de S3 deben ser únicos de forma global.
7. Seleccione Create.
8. Elija el registro de seguimiento `My-Test-Trail` que acaba de crear.
9. Seleccione el icono de lápiz junto a Management events.
10. Para Read/Write events, elija All, Save y, a continuación, elija Configure.

CloudWatch Events permite elegir entre diferentes maneras de enviar alertas cuando una regla de alarma coincide con una llamada a la API entrante. En este tutorial se muestran dos métodos: invocar una función Lambda que puede registrar la llamada a API y enviar información a un tema de Amazon SNS que, a su vez, envía un correo electrónico o mensaje de texto a los suscriptores del tema. En los próximos dos pasos, debe crear los componentes que necesita, la función Lambda y el tema de Amazon SNS.

Paso 2: Configuración de una función Lambda

En este paso, se crea una función Lambda que registra la actividad de API que le envía la regla de CloudWatch que configuraremos más adelante.

Para crear una función Lambda que registra eventos de CloudWatch Events

1. Abra la consola de AWS Lambda en https://console.aws.amazon.com/lambda/.
2. Si eres nuevo en Lambda, eligeIntroducción aEn la página de bienvenida; de lo contrario, elijaCrear una función.
3. En la página Create function, elija Blueprints.
4. En el cuadro de búsqueda Blueprints (Proyectos), escriba **`hello`** para el filtro y elija el proyecto hello-world.
5. Elija Configure (Configurar).
6. En la página Basic information (Información básica), haga lo siguiente:
   a. Para el nombre de la función Lambda, escriba**`LogOrganizationEvents`**en laNombre.
   b. ParaRol, elijaCreación de una función de personalizaday, a continuación, en la parte inferior delAWS LambdaRequiere acceso a los recursos de, elijaPermitir. Esta función concede a la función Lambda permisos para obtener acceso a los datos que requiere y para escribir en su registro de salida.
   c. Elija Create function (Crear función).
7. En la página siguiente, edite el código de la función Lambda, como se muestra en el ejemplo siguiente.

```
console.log('Loading function');

exports.handler = async (event, context) => {
    console.log('LogOrganizationsEvents');
    console.log('Received event:', JSON.stringify(event, null, 2));
    return event.key1;  // Echo back the first key value
    // throw new Error('Something went wrong');
};
```

   Este código de muestra registra el evento con una cadena de marcador **`LogOrganizationEvents`** seguida de la cadena JSON que compone el evento.
8. Seleccione Save.

Paso 3: Cree un tema de Amazon SNS que envía correos electrónicos a los suscriptores

En este paso, se crea un tema de Amazon SNS que envía información a sus suscriptores por correo electrónico. A continuación, este tema se convierte en «objetivo» de la regla de CloudWatch Events que se crea después.

Para crear un tema de Amazon SNS con el fin de enviar un correo electrónico a los suscriptores

1. Abra la consola de Amazon SNS enhttps://console.aws.amazon.com/sns/v3/.
2. En el panel de navegación, elija Topics (Temas).
3. Elija Create new topic (Crear nuevo tema).
   a. En Topic name (Nombre del tema), escriba **`OrganizationsCloudWatchTopic`**.

b. En Display name (Nombre visible), escriba **`OrgsCWEvnt`**.

c. Elija Create new topic (Crear nuevo nombre).

4. Ahora puede crear una suscripción para el tema. Elija el ARN del tema que acaba de crear.
5. Seleccione Create subscription (Crear suscripción).

   a. En la página Create subscription, para Protocol, elija Email.

   b. En Punto de enlace, introduzca su dirección de correo electrónico.

   c. Seleccione Create subscription (Crear suscripción). AWS envía un mensaje de correo electrónico a la dirección especificada en el paso anterior. Espere a recibir ese correo electrónico y, a continuación, elija el enlace Confirm subscription que contiene para confirmar que lo ha recibido correctamente.

   d. Vuelva a la consola y actualice la página. El mensaje Pending confirmation desaparece y se sustituye por el ID de suscripción que ha quedado validado.

Paso 4: Crear una regla de eventos de CloudWatch

Ahora que ya existe la función Lambda en su cuenta, debe crear una regla de CloudWatch Events que la invoque cuando se cumplan los criterios de dicha regla.

Para crear una regla de CloudWatch Events

1. Abra la consola de CloudWatch enhttps://console.aws.amazon.com/cloudwatch/.
2. Al igual que antes, debe configurar la consola en elEE.UU. Este (Norte de Virginia)La región o la información acerca de las Organizations no está disponible. En la barra de navegación de la esquina superior derecha de la consola, elija la opciónEE.UU. Este (Norte de Virginia)Región .
3. En el panel de navegación, elija Rules (Reglas) y, a continuación, seleccione Create rule (Crear regla).
4. En Event source, haga lo siguiente:

   a. Seleccione Event pattern.

   b. Seleccione Build event pattern to match events by service.

   c. En Service Name, elija Organizations.

   d. ParaTipo de evento, elijaAWSAPI llamada a través de CloudTrail.

   e. SeleccionarOperaciones específicasy, a continuación, indique las API que quiera monitorizar: CreateAccountyCreateOrganizationalUnit. Puede seleccionar también otras que también desee. Para obtener una lista completa de las API de AWS Organizations disponibles, consulte la AWS OrganizationsReferencia de la API de .
5. En Targets(Destinos), en Function (Función), elija la función que creó en el procedimiento anterior.
6. En Targets, seleccione Add target.
7. En la nueva fila de destino, elija el encabezado desplegable y, a continuación, seleccione SNS topic (Tema de SNS).
8. Para Topic (Tema), elija el tema denominado OrganizationCloudWatchTopic que haya creado en el procedimiento anterior.
9. Seleccione Configure details.
10. En la página Configure rule details (Configurar los detalles de la regla), en Name (Nombre), escriba **`OrgsMonitorRule`**, deje State (Estado) seleccionado y, a continuación, elija Create rule (Crear regla).

Paso 5: Prueba de la regla de CloudWatch Events

En este paso, se crea una unidad organizativa (OU) y se observa que la regla de CloudWatch Events genera una entrada de registro y envía un correo electrónico con información detallada sobre el evento.

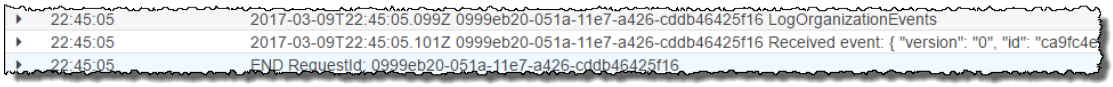
AWS Management Console

Para crear una unidad organizativa (OU)

1. Abra el iconoAWS Organizationsa la consola de Cuentas de AWS page.
2. Active la casilla de verificación RootOU, elijaActionsy, a continuación, enDependencia organizativaelijaCrear nuevos.
3. Para el nombre de la unidad organizativa, escriba **`TestCWEOU`** y, a continuación, elija Create organizational unit (Crear unidad organizativa).

Para ver la entrada de registro de CloudWatch Events

1. Abra la consola de CloudWatch enhttps://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija Logs (registros).
3. UNDERGrupos de registrosElija el grupo que está asociado a su función Lambda:/aws/Lambda/logOrganizationEvents.
4. Cada grupo contiene uno o más flujos; debería haber un grupo para hoy. Elíjalo.
5. Consulte el registro. Deben aparecer filas similares a las siguientes.



6. Seleccione la fila central de la entrada para ver todo el texto JSON del evento recibido. Aparecen todos los detalles de la solicitud al API en los componentes `requestParameters` y `responseElements` de la salida.

```
2017-03-09T22:45:05.101Z 0999eb20-051a-11e7-a426-cddb46425f16 Received event:
{
    "version": "0",
    "id": "123456-EXAMPLE-GUID-123456",
    "detail-type": "AWS API Call via CloudTrail",
    "source": "aws.organizations",
    "account": "123456789012",
    "time": "2017-03-09T22:44:26Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "eventVersion": "1.04",
        "userIdentity": {
            ...
        },
        "eventTime": "2017-03-09T22:44:26Z",
        "eventSource": "organizations.amazonaws.com",
        "eventName": "CreateOrganizationalUnit",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "192.168.0.1",
        "userAgent": "AWS Organizations Console, aws-internal/3",
        "requestParameters": {
            "parentId": "r-exampleRootId",
            "name": "TestCWEOU"
        },
        "responseElements": {
            "organizationalUnit": {
```

```
                "name": "TestCWEOU",
                "id": "ou-exampleRootId-exampleOUId",
                "arn": "arn:aws:organizations::1234567789012:ou/o-exampleOrgId/ou-
exampleRootId-exampeOUId"
            }
        },
        "requestID": "123456-EXAMPLE-GUID-123456",
        "eventID": "123456-EXAMPLE-GUID-123456",
        "eventType": "AwsApiCall"
    }
}
```

7. Consulte su cuenta de correo electrónico para ver el mensaje enviado porOrgsCwevnt(el nombre de visualización del tema de Amazon SNS). El cuerpo del correo electrónico contiene la misma salida de texto JSON que la entrada de registro mostrada en el paso anterior.

Limpieza: Elimine los recursos que ya no necesite

Para evitar que se acumulen cargos, debe eliminar todos los recursos de AWS creados durante este tutorial y que no desee conservar.

Para eliminar los recursos del entorno de AWS

1. Usarconsola de CloudTrailPara eliminar el registro de seguimiento llamado**`My-Test-Trail`**que creó en el paso 1.
2. Si ha creado un bucket de Amazon S3 en el paso 1, utilice laConsola de Amazon S3para eliminarlo.
3. UsarConsola de LambdaPara eliminar la función de llamada**`LogOrganizationEvents`**que creó en el paso 2.
4. UsarConsola de Amazon SNSpara eliminar el tema de Amazon SNS denominado**`OrganizationsCloudWatchTopic`**que creó en el paso 3.
5. Usarconsola de CloudWatchpara eliminar la regla de CloudWatch denominada**`OrgsMonitorRule`**que creó en el paso 4.
6. Por último, utilice la herramientaConsola de Organizationspara eliminar la unidad organizativa denominada**`TestCWEOU`**que creó en el paso 5.

Y ya está. En este tutorial, ha configurado CloudWatch Events para monitorear los cambios que puedan producirse en la organización. Ha configurado una regla que se activa cuando los usuarios invocan determinadas operaciones de AWS Organizations. La regla ha ejecutado una función Lambda que registró el evento y envió un correo electrónico que contenía información sobre dicho evento.

Prácticas recomendadas para AWS Organizations

Le recomendamos que siga estas prácticas recomendadas cuando cree y utilice su organización.

Temas

Prácticas recomendadas para la cuenta de

Siga estas recomendaciones para ayudar a proteger la seguridad de la cuenta de administración enAWS Organizations. Estas recomendaciones suponen que también se adhiere a laPráctica recomendada de utilizar el usuario raíz exclusivamente para aquellas tareas que realmente lo requieren.

> Note
>
> AWS Organizationsestá cambiando el nombre de la «cuenta maestra» a «cuenta de gestión». Solo se cambia el nombre y no se cambia su funcionalidad. Es posible que siga viendo algunas instancias del término anterior mientras completamos el trabajo para la transición al término más reciente. Si ves uno que nos perdimos, por favor usa elComentariosen la parte superior de esa página para hacernos saber.

Temas

Utilice la cuenta de administración sólo para tareas querequireCuenta de

Le recomendamos que utilice la cuenta de administración y sus usuarios y roles sólo para tareas que sólo puede realizar esa cuenta. Almacene todos susAWSrecursos enotros Cuentas de AWS en la organización y mantenerlos fuera de la cuenta de administración. La única excepción es que recomendamos que habiliteAWS CloudTraily mantener los rastros y registros relevantes de CloudTrail en la cuenta de administración.

Una razón importante para mantener los recursos en otras cuentas es porque las directivas de control de servicios (SCPs) de Organizations no funcionan para restringir ningún usuario o rol en la cuenta de administración.

Separar los recursos de su cuenta de gestión también le ayudará a comprender los cargos de sus facturas.

Usar una dirección de correo electrónico de grupo para el usuario raíz de la cuenta de administración

- Utilice una dirección de correo electrónico administrada por su empresa. No utilice un proveedor de correo electrónico público o uno que esté administrado por un tercero.
- Utilice una dirección de correo electrónico que reenvíe los mensajes recibidos directamente a una lista de gerentes empresariales sénior. En el caso de queAWSnecesita ponerse en contacto con el propietario de la cuenta, por ejemplo, para confirmar el acceso, el mensaje de correo electrónico se distribuye a varias partes. Este enfoque ayuda a reducir el riesgo de retrasos en la respuesta, incluso si las personas están de vacaciones, se enferman o abandonan el negocio.

Utilice una contraseña compleja para elUsuario raíz

- La seguridad de losUsuario raízdepende de la fuerza de su contraseña. Le recomendamos que utilice una contraseña larga, compleja y que no se utilice en ningún otro lugar. Numerosos administradores de contraseñas y complejos algoritmos y herramientas de generación de contraseñas pueden ayudarle a alcanzar estos objetivos.
- Si está utilizando una contraseña segura, como se describe en el punto anterior, y rara vez accede al usuario raíz, le recomendamos que haganoPeriódicamente cambie la contraseña. Cambiar la contraseña con más frecuencia de lo que usa aumenta el riesgo de comprometerse.
- Confíe en la política de seguridad de la información de su empresa para administrar el almacenamiento a largo plazo y el acceso a la contraseña del usuario raíz. Este enfoque puede significar que realice alguna de las siguientes acciones:
  - Imprima la contraseña y guárdela en una caja fuerte.
  - Divida la contraseña en pedazos y distribuya las piezas a los gerentes de negocios sénior.
  - Almacene la contraseña en un sistema o herramienta de administrador de contraseñas bajo controles y procesos adicionales. Si utiliza un administrador de contraseñas, le recomendamos que esté sin conexión. Para evitar crear una dependencia circular, no almacene la contraseña del usuario raíz con herramientas que dependen deAWSen los que inicia sesión con la cuenta protegida.

  Sea cual sea el método que elijas, te recomendamos que el método sea resistente y que requiera la participación de múltiples agentes para reducir los riesgos de colusión.
- Cualquier acceso a la contraseña o a su ubicación de almacenamiento debe registrarse y supervisarse.

Habilitar MFA para suUsuario raízcredenciales

Para obtener instrucciones sobre cómo habilitar la autenticación multifactor (MFA), consulteUso de la autenticación multifactor (MFA) enAWS.

- Utilice un dispositivo basado en hardware que no dependa de una batería para generar la contraseña de un solo uso (OTP). Este enfoque ayuda a garantizar que el MFA sea imposible de duplicar y que no esté sujeto a riesgos de desvanecimiento de la batería durante el almacenamiento a largo plazo.
  - Si decide utilizar un MFA basado en batería, asegúrese de agregar procesos para comprobar el dispositivo periódicamente y reemplazarlo cuando se acerque la fecha de caducidad.
  - Cree un plan para manejar la logística de la necesidad de mantener el acceso 24/7 al token en caso de que sea necesario.
- Le recomendamos queDon'treutilizar ese MFA físico para cualquier otro propósito que no sea proteger esta cuenta de administración. Si reutiliza el MFA físico, puede crear confusión operativa y exposición innecesaria del MFA.

- Almacene el dispositivo MFA de acuerdo con su política de seguridad de la información, peronoen el mismo lugar que la contraseña asociada para el usuario. Asegúrese de que el proceso para acceder a la contraseña y el proceso para acceder al MFA requieren un acceso diferente a diferentes recursos (personas, datos y herramientas).
- Cualquier acceso del dispositivo MFA o de su ubicación de almacenamiento debe registrarse y supervisarse.

Agregar un número de teléfono a la información de contacto de la cuenta

- Aunque hay algunos vectores de ataque creíbles contra números de teléfono fijo, SIP y teléfonos móviles, en general los riesgos se ven compensados por la complejidad de estos vectores. Si utiliza este mecanismo para recuperar el acceso raíz, hay otros factores disponibles para elAWS Supportrepresentante para gestionar estos riesgos. Por lo tanto, recomendamos agregar un número de teléfono como una barrera adicional útil para el proceso.
- Hay varias opciones para aprovisionar un número de teléfono, pero la que recomendamos es una tarjeta SIM dedicada y un teléfono, almacenados a largo plazo en una caja fuerte. Es importante asegurarse de que el equipo responsable del pago de la factura del móvil para este contrato telefónico comprenda la importancia del número aunque aparentemente no habrá llamadas enviadas o recibidas por él durante largos períodos de tiempo.
- Es importante que este número de teléfono no sea bien conocido dentro del negocio. Documentarlo en elAWSInformación de contactoy comparta sus detalles con su equipo de facturación. No lo documente en ningún otro lugar. Este enfoque ayuda a reducir el riesgo de los vectores de ataque asociados con mover el número de teléfono vinculado a la SIM a otra SIM.
- Almacene el teléfono de acuerdo con su política de seguridad de la información existente. Sin embargo, no almacene el teléfono en la misma ubicación que la otra información de credenciales relacionada.
- Cualquier acceso del teléfono o de su ubicación de almacenamiento debe registrarse y supervisarse.

Revisar y realizar un seguimiento de quién tiene acceso

- Para asegurarse de mantener el acceso a la cuenta de administración, revise periódicamente al personal de su empresa que tiene acceso a la dirección de correo electrónico, contraseña, MFA y número de teléfono asociados a ella. Alinee su revisión con los procedimientos comerciales existentes. Sin embargo, vale la pena agregar una revisión mensual o trimestral de esta información para asegurarse de que solo las personas correctas tengan acceso.
- Asegúrese de que el proceso para recuperar o restablecer el acceso a las credenciales del usuario raíz no dependa de que se complete ninguna persona específica. Todos los procesos deben abordar la posibilidad de que las personas no estén disponibles.

Documentar los procesos para usar las credenciales de usuario raíz

- Es común que los procesos importantes, como la creación de la cuenta de gestión de la organización, sean un proceso planificado que incluya varios pasos con múltiples personal. Se recomienda documentar y publicar ese plan, incluidos los pasos que se deben realizar y su secuencia de finalización. Este enfoque ayuda a garantizar que las decisiones tomadas se sigan correctamente.

- Documentar el rendimiento de procesos importantes a medida que se llevan a cabo para asegurarse de que tiene un registro de las personas involucradas en cada paso y de los valores utilizados. También es importante proporcionar documentación sobre las excepciones y eventos imprevistos que se produzcan.

  Si ocurre una excepción o un evento imprevisto, documente la hora en que ocurrió, quién salió de la sala y qué se sacó. A continuación, también debe documentar quién regresó a la habitación y lo que fue traído de vuelta.
- Cree un conjunto de procesos publicados acerca de cómo utilizar las credenciales de usuario raíz en diferentes escenarios, como restablecer la contraseña. Si no está seguro sobre el proceso para interactuar conAWS Supporten un escenario específico, cree un ticket de soporte para solicitar la orientación más reciente sobre cómo realizar esa tarea.

  Algunos escenarios que debe documentar incluyen los siguientes:
  - Acceder al usuario raíz para realizar una de las operaciones que solo el usuario raíz puede realizar.
  - Restablecer una contraseña de usuario raíz cuando pierda el acceso.
  - Cambiar la contraseña del usuario raíz cuando todavía tiene acceso.
  - Restablecer el usuario raíz MFA cuando pierde el acceso al dispositivo.
  - Cambiar el MFA del usuario raíz cuando se utiliza un dispositivo basado en batería.
  - Restablecer la dirección de correo electrónico del usuario raíz cuando pierda el acceso a la cuenta de correo electrónico.
  - Cambiar la dirección de correo electrónico del usuario raíz cuando todavía tiene acceso.
  - Restablecer el número de teléfono del usuario raíz cuando pierda el acceso al número de teléfono.
  - Cambiar el número de teléfono del usuario raíz cuando todavía tiene acceso.
  - Eliminar la cuenta de administración de la organización.
- Pruebe y valide que siga teniendo acceso al usuario raíz y que el número de teléfono móvil esté operativo al menos trimestralmente. Esta programación ayuda a asegurar al negocio que el proceso funciona y que usted mantiene el acceso. También demuestra que los custodios del acceso comprenden los pasos que necesitan realizar para que el proceso tenga éxito. Nunca quieres estar en una posición en la que el personal involucrado en un proceso no entienda lo que se supone que deben hacer. Al igual que con los simulacros de incendios, la práctica desarrolla competencia y reduce las sorpresas.

  Con cada prueba, aproveche la oportunidad para reflexionar sobre la experiencia y proponer mejoras en el proceso. Examine especialmente los pasos que se realizaron incorrectamente o dieron lugar a resultados inesperados. ¿Cómo podría cambiar el proceso para mejorarlo la próxima vez?

  Algunos clientes utilizan estas pruebas como una oportunidad para rotar contraseñas. Nuestra recomendación es no rotar contraseñas. En su lugar, mantenga la misma contraseña compleja. Solo debe considerar actualizar la contraseña si sospecha que está comprometida.

Aplicar controles para supervisar el acceso a las credenciales del usuario raíz

- El acceso a las credenciales de usuario raíz debe ser un evento raro. Cree alertas con herramientas como Amazon CloudWatch Events para anunciar el inicio de sesión y el uso de las credenciales de usuario raíz de la cuenta de administración. Este anuncio debe incluir, pero no debe limitarse a, la dirección de correo electrónico utilizada para el propio usuario root. Este anuncio debe ser significativo y difícil de perder, ya sea que el uso sea válido o malicioso. Para ver un ejemplo, consulte .Supervise y notifique en Cuenta de AWS Usuario raíz.
- Asegúrese de que el personal que recibe dicho anuncio entienda cómo validar que se espera el acceso del usuario raíz y cómo escalar si cree que un incidente de seguridad está en curso.

Prácticas recomendadas para cuentas de miembros

Siga estas recomendaciones para ayudar a proteger la seguridad de las cuentas de miembro de su organización. Estas recomendaciones suponen que también se adhiere a laPráctica recomendada de utilizar el usuario raíz únicamente para aquellas tareas que realmente lo requieran.

Temas

Usar una dirección de correo electrónico de grupo para todos los usuarios raíz de cuentas de miembro

- Utilice una dirección de correo electrónico administrada por su empresa. No utilice un proveedor de correo electrónico público o uno que sea administrado por un tercero.
- Utilice una dirección de correo electrónico que reenvíe los mensajes recibidos directamente a una lista de gerentes empresariales sénior. En el caso de queAWSnecesita ponerse en contacto con el propietario de la cuenta, por ejemplo, para confirmar el acceso, el correo electrónico se distribuye a varias partes. Este enfoque ayuda a reducir el riesgo de retrasos en la respuesta, incluso si las personas están de vacaciones, se enferman o abandonan el negocio.

Usar una contraseña compleja para la cuenta de miembroUsuario raíz

- La seguridad de losUsuario raízdepende de la fuerza de su contraseña. Le recomendamos que utilice una contraseña larga, compleja y que no se utilice en ningún otro lugar. Numerosos administradores de contraseñas y complejos algoritmos y herramientas de generación de contraseñas pueden ayudarle a alcanzar estos objetivos.
- Si está utilizando una contraseña segura, como se describe en el punto anterior, y rara vez accede al usuario raíz, le recomendamos que haganoCambie periódicamente la contraseña. Cambiar la contraseña con más frecuencia de lo que usa aumenta el riesgo de comprometerse.
- Confíe en la política de seguridad de la información de su empresa para administrar el almacenamiento a largo plazo y el acceso a las contraseñas de los usuarios raíz de su cuenta de miembro. Sin embargo, a diferencia de la cuenta de administración, es razonable considerar almacenar la contraseña en un sistema o herramienta de administrador de contraseñas creíble y aprobado por la empresa.

  Almacene la contraseña en un sistema o herramienta de administrador de contraseñas bajo controles y procesos adicionales. Si utiliza un administrador de contraseñas, le recomendamos que esté sin conexión. Para evitar crear una dependencia circular, no almacene la contraseña con herramientas que dependen deAWSen los que inicia sesión con la cuenta protegida.

Sea cual sea el método que elijas, te recomendamos que el método sea resistente y que requiera la participación de múltiples agentes para reducir los riesgos de colusión.

- Alternativamente, puede almacenar la contraseña de un usuario raíz de cuenta miembro en unutilizando la guía que proporcionamos para el usuario raíz de la cuenta de administración (p. 26).
- Considere no habilitar credenciales para el usuario raíz en las cuentas de miembro creadas. De forma predeterminada, las Organizations asignan una contraseña aleatoria, compleja y muy larga que no se puede recuperar. En su lugar, para acceder al usuario raíz, debe realizar los pasos para la recuperación de contraseña. Le recomendamos que no lo haga a menos que necesite realizar una tarea que solo puede realizar el usuario raíz en la cuenta. Para obtener más información, consulte Acceso a una cuenta miembro como usuario raíz (p. 67) .
- Sin embargo, elija manejar la contraseña del usuario raíz, puede aplicar una directiva de control de servicios (SCP) que impida que los usuarios raíz de la cuenta miembro llamen a cualquierAWSAPIs. Sin embargo, si necesita responder a un evento de seguridad significativo en una cuenta de miembro, es posible que necesite un acceso rápido al usuario raíz de esa cuenta. Por lo tanto, el uso de una contraseña compleja para el usuario raíz de la cuenta miembro y la creación de procedimientos de acceso y uso por adelantado sigue siendo el enfoque recomendado, como se describe en los puntos anteriores.

Habilitar MFA para suUsuario raízcredenciales

Para obtener instrucciones sobre cómo habilitar la autenticación multifactor (MFA), consulteUso de la autenticación multifactor (MFA) enAWS.

- Se recomienda utilizar un dispositivo basado en hardware que no dependa de una batería para generar la contraseña de un solo uso (OTP). Este enfoque ayuda a garantizar que el MFA sea imposible de duplicar y que no esté sujeto a riesgos de desvanecimiento de la batería durante el almacenamiento a largo plazo
  - Si decide utilizar un MFA basado en batería, asegúrese de agregar procesos para comprobar el dispositivo periódicamente y reemplazarlo cuando se acerque la fecha de caducidad.
  - Cree un plan para manejar la logística de la necesidad de mantener el acceso 24/7 al token en caso de que sea necesario.
- Si elige usar una aplicación MFA virtual, a diferencia de nuestrarecomendación para la cuenta de gestiónUsuario raíz (p. 26), para cuentas de miembro puede volver a utilizar un único dispositivo MFA para varias cuentas de miembro. Puede abordar las limitaciones geográficas imprimiendo y almacenando de forma segura el código QR utilizado para configurar la cuenta en la aplicación MFA virtual. Documentar el propósito del código QR y sellarlo y almacenarlo en cajas fuertes accesibles en todas las zonas horarias en las que opera, de acuerdo con su política de seguridad de la información. Luego, cuando se necesita acceso en una ubicación geográfica diferente, la copia local del código QR se puede recuperar y usar para configurar una aplicación MFA virtual en la nueva ubicación.
- Almacene el dispositivo MFA de acuerdo con su política de seguridad de la información, peronoen el mismo lugar que la contraseña asociada paraUsuario raíz. Asegúrese de que el proceso para acceder a la contraseña y el proceso para acceder al dispositivo MFA requieren diferentes procedimientos de acceso por diferentes recursos (personas, datos y herramientas).
- Cualquier acceso del dispositivo MFA o de su ubicación de almacenamiento debe registrarse y supervisarse.
- Si pierdes o rompes el dispositivo MFA, es posible que tengas que ponerte en contacto con el servicio de atención al Support para eliminar el MFA de tu cuenta. Antes de que puedan hacerlo, deben verificar que la persona que realiza la solicitud esté en posesión de la dirección de correo electrónico, el número de teléfono y las preguntas de seguridad asociadas a la cuenta. Así que asegúrese de tener esa información y mantenerla actualizada y almacenada de forma segura.

Agregar el número de teléfono de la cuenta de gestión a la información de contacto de la cuenta de miembro

- Por lo general, puede confiar en elnúmero de teléfono de la cuenta de administración de la organización (p. 27)para cualquier recuperación crítica de la cuenta. Por lo tanto, creemos que es una sobrecarga operativa innecesaria administrar un número de teléfono independiente a la información de contacto de una cuenta de miembro. Por lo tanto, le recomendamos agregar el mismo número de teléfono que la cuenta de administración. Independientemente de si utiliza o no el mismo número que la cuenta de administración, mantenga una lista precisa de los números de teléfono utilizados y cualquier pregunta de seguridad activa en una ubicación segura similar a las credenciales mismas.

Revisar y realizar un seguimiento de quién tiene acceso

- Como se recomienda para la cuenta de gestión (p. 27), debe revisar periódicamente al personal de su empresa que tiene acceso a la dirección de correo electrónico, contraseña, MFA y número de teléfono de su cuenta de miembroUsuario raíz. Alinee su revisión con los procedimientos comerciales existentes. Sin embargo, vale la pena agregar una revisión mensual o trimestral de esta información para asegurarse de que solo las personas correctas tengan acceso.
- Asegúrese de que el proceso para recuperar o restablecer el acceso a las credenciales del usuario raíz no dependa de que se complete ninguna persona específica. Todos los procesos deben abordar la posibilidad de que las personas no estén disponibles.

Documentar los procesos para usar las credenciales de usuario raíz

- Es común que los procesos importantes, como la creación de la cuenta de gestión de la organización, sean un proceso planificado que incluya varios pasos con múltiples personal. Se recomienda documentar y publicar ese plan, incluidos los pasos que se deben realizar y su secuencia de finalización. Este enfoque ayuda a garantizar que las decisiones tomadas se sigan correctamente.
- Documentar el rendimiento de procesos importantes a medida que se llevan a cabo para asegurarse de que tiene un registro de las personas involucradas en cada paso y de los valores utilizados. También es importante proporcionar documentación sobre las excepciones y eventos imprevistos que se produzcan.

  Si ocurre una excepción o un evento imprevisto, documente la hora en que ocurrió, quién salió de la sala y qué se sacó. A continuación, también debe documentar quién regresó a la habitación y lo que fue traído de vuelta.
- Cree y publique procesos acerca de cómo usar elUsuario raízen diferentes escenarios, como restablecer la contraseña. Si no está seguro sobre el proceso para interactuar conAWS Supporten un escenario específico, cree un ticket de soporte para solicitar la orientación más reciente sobre cómo realizar esa tarea.

  Algunos de los escenarios que debe documentar incluyen lo siguiente:
  - Acceder al usuario raíz para realizar una de las operaciones que solo el usuario raíz puede realizar.
  - Restablecer una contraseña de usuario raíz cuando pierda el acceso.
  - Cambiar la contraseña del usuario raíz cuando todavía tiene acceso.
  - Restablecer el MFA del usuario raíz cuando pierda el acceso al dispositivo.
  - Cambiar el MFA del usuario raíz cuando se utiliza un dispositivo basado en batería.

- Restablecer la dirección de correo electrónico del usuario raíz cuando pierda el acceso a la cuenta de correo electrónico.
- Cambiar la dirección de correo electrónico del usuario raíz cuando todavía tiene acceso.
- Restablecer el número de teléfono del usuario raíz cuando pierda el acceso al número de teléfono.
- Cambiar el número de teléfono del usuario raíz cuando todavía tiene acceso.
- Eliminar la cuenta de administración de la organización.

- Pruebe y valide que siga teniendo acceso al usuario raíz y que el número de teléfono móvil de la cuenta de miembro (si ha asignado una) esté operativo al menos trimestralmente. Esta programación ayuda a asegurar al negocio que el proceso funciona y que usted mantiene el acceso. También demuestra que los custodios del acceso comprenden los pasos que necesitan realizar para que el proceso tenga éxito. Nunca quieres estar en una posición en la que el personal involucrado en un proceso no entienda lo que se supone que deben hacer. Al igual que con los simulacros de incendios, la práctica desarrolla competencia y reduce las sorpresas.

  Con cada prueba, aproveche la oportunidad para reflexionar sobre la experiencia y proponer mejoras en el proceso. Examine especialmente los pasos que se realizaron incorrectamente o que dieron lugar a resultados inesperados. ¿Cómo podría cambiar el proceso para mejorarlo la próxima vez?

  Algunos clientes utilizan estas pruebas como una oportunidad para rotar contraseñas. Nuestra recomendación es no hacer esto, y mantener la misma contraseña compleja. Solo debe buscar actualizar la contraseña si sospecha que está comprometida.

Utiliza un SCP para restringir lo que puede hacer el usuario raíz en tus cuentas de miembro

Se recomienda crear una directiva de control de servicios (SCP) en la organización y adjuntarla a la raíz de la organización para que se aplique a todas las cuentas miembros. El siguiente ejemplo SCP impide que el usuario raíz de cualquier cuenta de miembro pueda crear cualquierAWSServicio de llamadas a la API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "StringLike": { "aws:PrincipalArn": "arn:aws:iam::*:root" }
            }
        }
    ]
}
```

En la mayoría de las circunstancias, cualquier tarea administrativa puede ser realizada por unAWS Identity and Access Management(IAM) en la cuenta de miembro que tiene permisos de administrador relevantes. Cualquiera de estos roles debe tener controles adecuados aplicados que limiten, registren y supervisen la actividad.

Aplicar controles para supervisar el acceso a las credenciales del usuario raíz

- Si elige habilitar el acceso a las credenciales del usuario raíz, dicho acceso debería ser un evento raro. Cree alertas con herramientas como Amazon CloudWatch Events para anunciar el inicio de sesión y el

uso de las credenciales de usuario raíz. Este anuncio debe ser significativo y difícil de perder, ya sea que el uso sea válido o malicioso. Para ver un ejemplo, consulte .Supervise y notifique en Cuenta de AWS Actividad de usuario raíz.

- Asegúrese de que el personal que recibe dicho anuncio entienda cómo validar que se espera el acceso del usuario raíz y cómo escalar si cree que un incidente de seguridad está en curso.

Creación y administración de una organización

Puede llevar a cabo las tareas siguientes a través deAWS Organizationso ejecutando unAWS Command Line Interface(AWS CLI) o el comando equivalenteAWSOperaciones de SDK:

- Crear una organización (p. 34). Cree una organización con su cuenta actual como cuenta de administración. Cree cuentas miembro en su organización e invite a otras cuentas a que se unan a su organización.
- Habilitar todas las características en la organización (p. 37). Habilitar todas las características es la forma idónea de trabajar con AWS Organizations. Al crear una organización, tiene la opción de habilitar todas las características o un subconjunto de ellas para unificar la facturación. Habilitar todas las características es la opción predeterminada e incluye las características de facturación unificada.

  Si están habilitadas todas las características, puede utilizar las de administración avanzada de cuentas disponibles en AWS Organizations, tales como las políticas de control de servicios (SCP) (p. 108). Las SCP ofrecen control centralizado de los máximos permisos disponibles para todas las cuentas de la organización. Esto le ayuda a mantener sus cuentas dentro de las directrices de control de acceso de la organización.
- Ver información detallada de su organización (p. 45). Vea información detallada de su organización y sus nodos raíz, unidades organizativas y cuentas.
- Eliminar una organización (p. 51). Elimine una organización cuando ya no la necesite.

> Note
>
> En los procedimientos de esta sección se indican los permisos mínimos necesarios para llevar a cabo las tareas. Estos se aplican normalmente a la API o al acceso a la herramienta de línea de comandos.
> Para realizar una tarea en la consola podría necesitar permisos adicionales. Por ejemplo, puede otorgar permisos de solo lectura a todos los usuarios de su organización y, a continuación, conceder otros permisos que permitan seleccionar los usuarios que pueden realizar tareas específicas.

Creación de una organización

Puede crear una organización comenzando por su Cuenta de AWS como cuenta de gestión. Cuando crea una organización, puede elegir si la organización admitirá todas las características (opción recomendada) o solo las de facturación unificada.

Después de crear una organización, puede añadir cuentas desde la cuenta de administración tal y como se indica a continuación:

- Crear otro Cuentas de AWS (p. 63)que se incorporen automáticamente a la organización como cuentas de miembro
- Después de verificar la dirección de correo electrónico,Invitar a existentes Cuentas de AWS (p. 55)Para que se una a su organización como miembros de cuentas

Creación de una organización

Puede crear una organización mediante laAWS Management Consoleo mediante un comando delAWS CLIo una de las API de SDK.

Permisos mínimos

Para crear una organización con la actual Cuenta de AWS Debe disponer de los siguientes permisos:

- `organizations:CreateOrganization`
- `iam:CreateServiceLinkedRole`

  Puede restringir este permiso solo a la entidad principal del servicio `organizations.amazonaws.com`.

AWS Management Console

Para crear una organización de

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. De forma predeterminada, la organización se crea con todas las características habilitadas. Sin embargo, puede elegir cualquiera de los pasos siguientes:

   - Para crear una organización con todas las características habilitadas, en la página de introducción, elijaCreación de una organización.
   - Para crear una organización con funciones de facturación consolidada únicamente, en la página de introducción y enCreación de una organización, elijaFunciones de facturación unificaday, a continuación, en el cuadro de diálogo de confirmación, elijaCreación de una organización.

   Si elige accidentalmente la opción equivocada, puede ir inmediatamente a laConfiguracióny, a continuación, elijaEliminar organizacióny empezar de nuevo.
3. Se crea la organización y la Cuentas de AWS Aparece una página. La única cuenta presente es su cuenta de administración, y actualmente está almacenada en elUnidad organizativa raíz (OU) (p. 6).

   Si es necesario, las Organizations envían automáticamente un correo electrónico de verificación a la dirección asociada a la cuenta de administración. Puede pasar algún tiempo hasta que reciba el correo electrónico de verificación. Verifique la dirección de correo electrónico en un plazo de 24 horas. Para obtener más información, consulte Verificación de dirección de correo electrónico (p. 36) . Puede crear cuentas para hacer crecer la organización sin verificar la dirección de correo electrónico de la cuenta de administración. Sin embargo, para invitar a otras cuentas existentes, primero debe completar la verificación de correo electrónico.

   Note

   Si esta cuenta ha verificado previamente su dirección de correo electrónico, no volverá a ocurrir cuando utilice la cuenta para crear una organización.

AWS CLI & AWS SDKs

Para crear una organización de

Puede utilizar uno de los siguientes comandos para crear una organización:

- AWS CLI:Create-organization

  En el ejemplo siguiente se crea una organización y se crea la Cuenta de AWS la cuenta de gestión de la organización.

```
$ aws organizations create-organization
{
    "Organization": {
        "Id": "o-aa111bb222",
        "Arn": "arn:aws:organizations::123456789012:organization/o-aa111bb222",
        "FeatureSet": "ALL",
        "MasterAccountArn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
        "MasterAccountId": "123456789012",
        "MasterAccountEmail": "admin@example.com",
        "AvailablePolicyTypes": [  ...DEPRECATED - DO NOT USE ... ]
    }
}
```

  Important

  La`AvailablePolicyTypes`está en desuso y no contiene información precisa sobre las directivas habilitadas en su organización. Para ver la lista precisa y completa de los tipos de directiva que están realmente habilitados para la organización, utilice la herramienta`ListRoots`, tal y como se describe en elAWS CLIEn la siguiente sección.

- AWSSDK: CreateOrganization

Ahora puede agregar cuentas adicionales a la organización tal y como se indica a continuación:

- Para crear un Cuenta de AWS que automáticamente se convierte en parte de suAWSorganización, consulteCreación de un Cuenta de AWS En su organización (p. 63).
- Para invitar a una cuenta existente a la organización, consulte Invitar a Cuenta de AWS Para unirse a su organización (p. 54).

Verificación de dirección de correo electrónico

Después de crear la organización, para poder invitar a otras cuentas a que se unan, debe verificar que es el propietario de la dirección de correo electrónico asociada a la cuenta de administración de la organización.

Al crear una organización, si la cuenta de administración no se ha verificado previamente,AWSEnviará automáticamente un correo electrónico de verificación a la dirección de correo electrónico especificada. Puede pasar algún tiempo hasta que reciba el correo electrónico de verificación.

En un plazo de 24 horas, siga las instrucciones del correo electrónico para verificar la dirección de correo electrónico.

Si no verifica la dirección de correo electrónico en un plazo de 24 horas, puede volver a enviar la solicitud de verificación, de modo que pueda invitar a otros Cuentas de AWS A la organización. Si no recibe el correo electrónico de verificación, compruebe que la dirección de correo electrónico es correcta y, si es necesario, modifíquela.

- Para saber qué dirección de correo electrónico está asociada a la cuenta de administración, consulteConsultar los detalles de una organización desde la cuenta de administración (p. 45).
- Para cambiar la dirección de correo electrónico asociada a la cuenta de administración, consulteAdministración de una Cuenta de AWS en laAWS Billing and Cost ManagementGuía del usuario de.

AWS Management Console

Para volver a enviar la solicitud de verificación

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. Vaya a la .Configuracióny, a continuación, elijaSolicitud de envío de verificación. La opción solo está presente si no se verifica la cuenta de administración.
3. Verifique la dirección de correo electrónico en un plazo de 24 horas.

   Después de verificar la dirección de correo electrónico, puede invitar a otros Cuentas de AWS A la organización. Para obtener más información, consulte Invitar a Cuenta de AWS Para unirse a su organización (p. 54) .

Si cambia la dirección de correo electrónico de la cuenta de administración, el estado de la cuenta volverá a ser «email unverified» (correo electrónico sin verificar) y deberá completar el proceso de verificación de la nueva dirección de correo electrónico.

Note

Si invitaste a las cuentas a unirse a tu organización antes de cambiar la dirección de correo electrónico de la cuenta de administración y esas invitaciones aún no han sido aceptadas, no se podrán aceptar hasta que verifiques la nueva dirección de correo electrónico de la cuenta de administración. Utilice el procedimiento anterior para volver a enviar la solicitud de verificación. Después de completar el proceso respondiendo al correo electrónico, sus cuentas invitadas pueden aceptar las invitaciones.

Habilitar todas las características en la organización

AWS Organizations tiene dos conjuntos de características disponibles:

- Todas las características (p. 7)— Este conjunto de características es la forma preferida de trabajar con.AWS Organizations, e incluye funciones de Consolidación de Facturación. Al crear una organización, las características se habilitan de manera predeterminada. Si están habilitadas todas las características, puede utilizar las de administración avanzada de cuentas disponibles enAWS Organizationstales comoadmite la integración con.AWSservices (p. 237)ydirectivas de administración de la organización (p. 86).
- Funciones de facturación unificada (p. 7)Todas las organizaciones admiten este subconjunto de características, que proporciona herramientas de administración básicas que puede utilizar para administrar de forma centralizada las cuentas de su organización.

Si crea una organización que solo tenga las características de facturación unificada, podrá habilitar posteriormente todas las características. En esta página se describe el proceso para habilitar todas las características.

Antes de habilitar todas las características

Antes de cambiar de una organización que admite solamente las características de facturación unificada a una organización que admita todas las características, tenga en cuenta lo siguiente:

- Cuando comienza el proceso para habilitar todas las características, AWS Organizations envía una solicitud a cada cuenta a la que ha invitado a unirse a su organización. Cada cuenta invitada debe aprobar la habilitación de todas las características aceptando la solicitud. Solo entonces podrá completar el proceso para habilitar todas las características en su organización. Si una cuenta rechaza la solicitud,

debe eliminar la cuenta de su organización o volver a enviar la solicitud. Se debe aceptar la solicitud antes de que pueda completar el proceso para habilitar todas las características. Las cuentas que ha creado utilizando AWS Organizations no reciben una solicitud porque no necesitan aprobar el control adicional.

- Puede seguir invitando cuentas a su organización mientras habilita todas las funciones. La invitación informa al propietario de una cuenta invitada si se está uniendo a una organización con solo facturación consolidada o con todas las funciones habilitadas.
  - Si invitas a una cuentaDuranteel proceso para habilitar todas las características, la invitación indica que la organización a la que se unen tiene todas las características habilitadas. Si cancela el proceso para habilitar todas las funciones antes de que la cuenta acepte la invitación, dicha invitación se cancelará. Debe invitar a la cuenta de nuevo para que sea miembro de una organización con solo características de facturación unificada.
  - Si invitas a una cuenta y la invitación aún no está aceptadaAntesinicia el proceso para habilitar todas las funciones, esa invitación se cancela porque la invitación indica que la organización sólo tiene funciones de facturación consolidadas. Debe invitar a la cuenta de nuevo para que sea miembro de una organización con todas las características habilitadas.
- También puede seguir creando cuentas en la organización. Ese proceso no se ve afectado por este cambio.
- AWS Organizationsverifica que todas las cuentas miembro tengan una función vinculada al servicio denominada`AWSServiceRoleForOrganizations`. Este rol es obligatorio en todas las cuentas para habilitar todas las características. Si elimina el rol en una cuenta invitada, al aceptar la invitación para habilitar todas las características, se vuelve a crear el rol. Si elimina la función en una cuenta creada en AWS Organizations, esa cuenta recibe una invitación específicamente para volver a crear la función. Todas estas invitaciones deben aceptarse para que la organización complete el procedimiento de habilitación de todas las características.
- Dado que habilitar todas las características permite utilizar SCP (p. 108), asegúrese de que los administradores de su cuenta comprendan los efectos de asociar SCP a la organización, las unidades organizativas o las cuentas. Las SCP pueden restringir lo que los usuarios e incluso los administradores pueden hacer en las cuentas afectadas. Por ejemplo, la cuenta de administración puede aplicar SCP que impidan a las cuentas miembro abandonar la organización.
- La cuenta de administración no se ve afectada por ninguna SCP. No puede limitar lo que los usuarios y roles de la cuenta de administración pueden hacer mediante la aplicación de SCP. Las políticas SCP afectan únicamente a las cuentas miembro.
- La migración desde las características de facturación unificada a todas las características es unidireccional. No puede revertir una organización con todas las características habilitadas a solo características de facturación unificada.
- (No recomendado) Si en su organización solo están habilitadas las características de facturación unificada, los administradores de la cuenta miembro pueden elegir eliminar el rol vinculado al servicio denominado`AWSServiceRoleForOrganizations`. Si en otro momento elige habilitar todas las características de una organización, este rol es necesario y se vuelve a crear en todas las cuentas como parte de la aceptación de la invitación para habilitar todas las características. Para obtener más información acerca de cómo AWS Organizations utiliza esta función, consulte AWS Organizations y roles vinculados al servicio (p. 236).

Comienzo del proceso para habilitar todas las características

Puede iniciar el proceso para habilitar todas las características iniciando sesión en la cuenta de administración de la organización. Para ello, siga los pasos que se describen a continuación.

Permisos mínimos

Para habilitar todas las características en su organización, debe contar con el permiso siguiente:

- `organizations:EnableAllFeatures`
- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations

AWS Management Console

Para pedir a las cuentas miembro invitadas que acepten la habilitación de todas las características en la organización

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaConfiguraciónpágina elegirIniciar proceso.
3. En la páginaHabilite todas las característicasConfirme que entiende que no puede volver a solo las características de facturación unificada una vez que realice el cambio eligiendo.Iniciar proceso.

   AWS Organizations envía una solicitud a cada cuenta invitada (no creada) de la organización para pedir que apruebe la habilitación de todas las características en la organización.
   Si tiene alguna de las cuentas que se han creado utilizando AWS Organizations y el administrador de la cuenta miembro eliminó la función vinculada al servicio denominada `AWSServiceRoleForOrganizations`, AWS Organizations envía a esa cuenta una solicitud para volver a crear la función.

   La consola muestra el cuadro de diálogoEstado de las solicitudes de aprobaciónpara las cuentas invitadas.

   Tip

   Para volver a esta página más adelante, abra elConfiguracióny en el cuadro de diálogoSolicitud enviadadate, elija.Ver estado.
4. LaHabilite todas las característicasmuestra el estado de las solicitudes de cada cuenta de la organización. Las cuentas que han aceptado la solicitud muestran el estado deACEPTADA. Las cuentas que aún no han acordado muestran un estado deOPEN.

AWS CLI & AWS SDKs

Para pedir a las cuentas miembro invitadas que acepten la habilitación de todas las características en la organización

Puede utilizar uno de los siguientes comandos para habilitar todas las características de una organización:

- AWS CLI:Habilitar todas las características

  El siguiente comando inicia el proceso para habilitar todas las características de la organización.

```
$ aws organizations enable-all-features
{
    "Handshake": {
        "Id": "h-79d8f6f114ee4304a5e55397eEXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-79d8f6f114ee4304a5e55397eEXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            }
```

```
        ],
        "State": "REQUESTED",
        "RequestedTimestamp": "2020-11-19T16:21:46.995000-08:00",
        "ExpirationTimestamp": "2021-02-17T16:21:46.995000-08:00",
        "Action": "ENABLE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "o-a1b2c3d4e5",
                "Type": "ORGANIZATION"
            }
        ]
    }
}
```


El resultado muestra los detalles del apretón de manos que las cuentas de miembro invitadas deben aceptar.

- AWSSDK: EnableAllFeatures

Notes

- Cuando se envía la solicitud a las cuentas miembro comienza una cuenta atrás de 90 días. Todas las cuentas deben aprobar la solicitud en ese período de tiempo; en caso contrario, la solicitud caducará. Si la solicitud expira, todas las solicitudes relacionadas con este intento se cancelan y tendrá que empezar con el paso 2.
- Durante el momento entre el que se realiza la solicitud para habilitar todas las características y cuando todas las cuentas aceptan la solicitud o se agota el tiempo de espera, todas las invitaciones pendientes para que otras cuentas se unan a la organización se cancelan automáticamente. No puede enviar nuevas invitaciones hasta que termine el proceso de activación de todas las características.
- Después de completar el proceso de activación de todas las características, puede invitar de nuevo a las cuentas a que se unan a la organización. El proceso no cambia, pero todas invitaciones incluyen información que permite a los destinatarios saber que si aceptan la invitación se regirán por las políticas aplicables.

Después de que todas las cuentas invitadas de la organización aprueben sus solicitudes, puede finalizar el proceso y habilitar todas las características. También puede finalizar inmediatamente el proceso si su organización no tiene ningunaInvitadoCuentas de miembros de. Para finalizar el proceso, continúe conFinalización del proceso para habilitar todas las características (p. 43).

Aprobación de la solicitud para habilitar todas las características o volver a crear el rol vinculado al servicio

Si inicias sesión en una de las cuentas miembro invitadas de la organización, puedes aprobar una solicitud desde la cuenta de administración. Si su cuenta recibió originalmente una invitación a unirse a la organización, la invitación es para habilitar todas las características y e incluye implícitamente la aprobación para recrear el rol `AWSServiceRoleForOrganizations`, si es necesario. Si su cuenta se ha creado en AWS Organizations y ha eliminado la función vinculada al servicio `AWSServiceRoleForOrganizations`, recibirá una invitación únicamente para volver a crear la función. Para ello, siga los pasos que se describen a continuación.

Important

Si realiza los pasos que se indican en el siguiente procedimiento, la cuenta de administración de la organización puede aplicar controles basados en políticas a la cuenta miembro. Estos controles

pueden restringir lo que los usuarios e incluso usted como administrador pueden hacer en la cuenta. Estas restricciones podrían impedir que su cuenta abandonara la organización.

Permisos mínimos

Para aprobar una solicitud para habilitar todas las características para la cuenta miembro, debe contar con los permisos siguientes:

- `organizations:AcceptHandshake`
- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:ListHandshakesForAccount`: solo se requiere cuando se utiliza la consola de Organizations
- `iam:CreateServiceLinkedRole`: solo se requiere si el`AWSServiceRoleForOrganizations`debe crearse de nuevo en la cuenta miembro de.

AWS Management Console

Para aceptar la solicitud para habilitar todas las características de la organización

1. Inicie sesión en el AWS Organizationsconsola de enAWS Organizationsconsole. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en una cuenta miembro.
2. Lea las implicaciones de aceptar la solicitud de todas las características para su cuenta y después elija Aceptar. La página muestra el proceso como incompleto hasta que todas las cuentas de la organización aceptan las solicitudes y el administrador de la cuenta administración finaliza el proceso.

AWS CLI & AWS SDKs

Para aceptar la solicitud para habilitar todas las características de la organización

Para aceptar la solicitud, debe aceptar el protocolo de enlace con `"Action": "APPROVE_ALL_FEATURES"`.

- AWS CLI:
  - Aceptar apretón de manos
  - lista-handshakes-for-account

  En el siguiente ejemplo de la se muestra cómo mostrar los enlaces de enlace disponibles para la cuenta de. El valor de`"Id"`en la cuarta línea de la salida es el valor que necesita para el siguiente comando.

```
$ aws organizations list-handshakes-for-account
{
    "Handshakes": [
        {
            "Id": "h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
            "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
approve_all_features/h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
            "Parties": [
                {
                    "Id": "a1b2c3d4e5",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "111122223333",
                    "Type": "ACCOUNT"
```

```
                }
            ],
            "State": "OPEN",
            "RequestedTimestamp": "2020-11-19T16:35:24.824000-08:00",
            "ExpirationTimestamp": "2021-02-17T16:35:24.035000-08:00",
            "Action": "APPROVE_ALL_FEATURES",
            "Resources": [
                {
                    "Value": "c440da758cab44068cdafc812EXAMPLE",
                    "Type": "PARENT_HANDSHAKE"
                },
                {
                    "Value": "o-aa111bb222",
                    "Type": "ORGANIZATION"
                },
                {
                    "Value": "111122223333",
                    "Type": "ACCOUNT"
                }
            ]
        }
    ]
}
```

En el siguiente ejemplo se utiliza el Id del protocolo de enlace del comando anterior para aceptar ese protocolo de enlace.

```
$ aws organizations accept-handshake --handshake-id h-
a2d6ecb7dbdc4540bc788200aEXAMPLE
{
    "Handshake": {
        "Id": "h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
approve_all_features/h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "111122223333",
                "Type": "ACCOUNT"
            }
        ],
        "State": "ACCEPTED",
        "RequestedTimestamp": "2020-11-19T16:35:24.824000-08:00",
        "ExpirationTimestamp": "2021-02-17T16:35:24.035000-08:00",
        "Action": "APPROVE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "c440da758cab44068cdafc812EXAMPLE",
                "Type": "PARENT_HANDSHAKE"
            },
            {
                "Value": "o-aa111bb222",
                "Type": "ORGANIZATION"
            },
            {
                "Value": "111122223333",
                "Type": "ACCOUNT"
            }
        ]
    }
```

```
}
```

- AWSSDK:
  - lista-handshakes-for-account
  - AcceptHandshake

Finalización del proceso para habilitar todas las características

Todas las cuentas miembro invitadas deben aprobar la solicitud para habilitar todas las características. Si no hay ninguna cuenta miembro invitada en la organización, la página Enable all features progress (Progreso de habilitación de todas las características) indica con un banner verde que puede finalizar el proceso.

Permisos mínimos

Para finalizar el proceso para habilitar todas las características de la organización, debe contar con el permiso siguiente:

- `organizations:AcceptHandshake`
- `organizations:ListHandshakesForOrganization`
- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations

AWS Management Console

Para finalizar el proceso para habilitar todas las características

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaConfiguraciónSi todas las cuentas invitadas aceptan la solicitud para habilitar todas las características, aparecerá un cuadro verde situado en la parte superior de la página para informarle. En el cuadro verde, elija.Ir a finalizar.
3. En la páginaHabilite todas las características, elijaFINALIZEy, a continuación, en el cuadro de diálogo de confirmación, elija.FINALIZEde nuevo.
4. Ahora, la organización tiene habilitadas todas las características.

AWS CLI & AWS SDKs

Para finalizar el proceso para habilitar todas las características

Para completar el proceso, debe aceptar el protocolo de enlace con `"Action": "ENABLE_ALL_FEATURES"`.

- AWS CLI:
  - List-handshakes-for-organization
  - Aceptar apretón de manos

```
$ aws organizations list-handshakes-for-organization
{
    "Handshakes": [
        {
            "Id": "h-43a871103e4c4ee399868fbf2EXAMPLE",
```

```
            "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-43a871103e4c4ee399868fbf2EXAMPLE",
            "Parties": [
                {
                    "Id": "a1b2c3d4e5",
                    "Type": "ORGANIZATION"
                }
            ],
            "State": "OPEN",
            "RequestedTimestamp": "2020-11-20T08:41:48.047000-08:00",
            "ExpirationTimestamp": "2021-02-18T08:41:48.047000-08:00",
            "Action": "ENABLE_ALL_FEATURES",
            "Resources": [
                {
                    "Value": "o-aa111bb222",
                    "Type": "ORGANIZATION"
                }
            ]
        }
    ]
}
```

En el ejemplo siguiente se indica cómo enumerar los enlaces de enlace disponibles para la organización. El valor de`"Id"`en la cuarta línea de la salida es el valor que necesita para el siguiente comando.

```
$ aws organizations accept-handshake \
    --handshake-id h-43a871103e4c4ee399868fbf2EXAMPLE
{
    "Handshake": {
        "Id": "h-43a871103e4c4ee399868fbf2EXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-43a871103e4c4ee399868fbf2EXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            }
        ],
        "State": "ACCEPTED",
        "RequestedTimestamp": "2020-11-20T08:41:48.047000-08:00",
        "ExpirationTimestamp": "2021-02-18T08:41:48.047000-08:00",
        "Action": "ENABLE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "o-aa111bb222",
                "Type": "ORGANIZATION"
            }
        ]
    }
}
```

- AWSSDK:
  - AcceptHandshake
  - AcceptHandshake

Los siguientes pasos:

- Habilite los tipos de políticas que desea utilizar. A partir de ese punto, puede adjuntar políticas para administrar las cuentas de su organización. Para obtener más información, consulte Administración de políticas de AWS Organizations (p. 86).

- Habilite la integración con los servicios compatibles. Para obtener más información, consulte Uso de AWS Organizations con otros servicios de AWS. (p. 232).

Consultar detalles de su organización

Puede realizar las siguientes tareas para ver los detalles de los elementos de su organización.

Temas

Consultar los detalles de una organización desde la cuenta de administración

Cuando inicia sesión en la cuenta de administración de la organización en elAWS Organizationsconsole Puede ver los detalles de la organización.

Permisos mínimos

Para ver los detalles de una organización, debe contar con el permiso siguiente:

- `organizations:DescribeOrganization`

AWS Management Console

Para ver los detalles de su organización

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. Vaya a la .Configuración(Se ha creado el certificado). Esta página muestra información acerca de la organización, incluido el ID de organización, el nombre de cuenta y la dirección de correo electrónico asignados a la cuenta de administración de la organización.

AWS CLI & AWS SDKs

Para ver los detalles de su organización

Puede utilizar uno de los siguientes comandos para ver detalles de una organización:

- AWS CLI:Describe-organization

  El siguiente ejemplo muestra la información incluida en el resultado de este comando.

```
$ aws organizations describe-organization
{
    "Organization": {
        "Id": "o-aa111bb222",
        "Arn": "arn:aws:organizations::123456789012:organization/o-aa111bb222",
```

```
        "FeatureSet": "ALL",
        "MasterAccountArn": "arn:aws:organizations::128716708097:account/o-
aa111bb222/123456789012",
        "MasterAccountId": "123456789012",
        "MasterAccountEmail": "admin@example.com",
        "AvailablePolicyTypes": [ ...DEPRECATED - DO NOT USE... ]
    }
}
```

Important

La`AvailablePolicyTypes`está en desuso y no contiene información precisa sobre las directivas habilitadas en su organización. Para ver la lista precisa y completa de los tipos de directiva que están realmente habilitados para la organización, utilice la herramienta`ListRoots`, como se describe en el comandoAWS CLIParte de la siguiente sección.

- AWSSDK: DescribeOrganization

Visualización de los detalles de la raíz

Cuando inicia sesión en la cuenta de administración de la organización en elAWS Organizationsconsole Puede ver los detalles de la raíz.

Permisos mínimos

Para ver los detalles de la raíz, debe contar con los siguientes permisos:

- `organizations:DescribeOrganization` (solo consola)
- `organizations:ListRoots`

La raíz es el contenedor superior de la jerarquía de unidades organizativas (OU) y generalmente se comporta como una unidad organizativa. Sin embargo, como el contenedor en la parte superior de la jerarquía, los cambios en la raíz afectan a todas las demás OU y cada Cuenta de AWS En la organización.

AWS Management Console

Para ver los detalles de la raíz

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. Vaya a la . Cuentas de AWS y elija la opciónRootOU (su nombre, no el botón de opción).
3. LaRootAparece la página de detalles y muestra los detalles de la raíz.

AWS CLI & AWS SDKs

Para ver los detalles de la raíz

Puede utilizar uno de los siguientes comandos para ver detalles de un nodo raíz:

- AWS CLI:list-roots

  En el siguiente ejemplo se muestra cómo recuperar los detalles de la raíz, incluidos los tipos de directiva que están habilitados actualmente en la organización:

```
$ aws organizations list-roots
```

```
{
    "Roots": [
        {
            "Id": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "PolicyTypes": [
                {
                    "Type": "BACKUP_POLICY",
                    "Status": "ENABLED"
                }
            ]
        }
    ]
}
```

- AWSSDK: ListRoots

Consultar los detalles de una unidad organizativa

Cuando inicia sesión en la cuenta de administración de la organización en elAWS Organizationsconsolepuede ver los detalles de las unidades organizativas de su organización.

Permisos mínimos

Para ver los detalles de una unidad organizativa, debe contar con los permisos siguientes:

- `organizations:DescribeOrganizationalUnit`
- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:ListOrganizationsUnitsForParent`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:ListRoots`: solo se requiere cuando se utiliza la consola de Organizations

AWS Management Console

Para ver detalles de una unidad organizativa

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la página Cuentas de AWS Elija el nombre de la unidad organizativa (no su botón de opción) que desea examinar. Si la unidad organizativa es una unidad secundaria de otra unidad organizativa, elija el icono del triángulo situado junto a su unidad organizativa principal para expandirla y ver las del siguiente nivel de la jerarquía. Repita hasta encontrar la unidad organizativa que desea.

   LaDetalles de la unidad organizativamuestra la información sobre la unidad organizativa.

AWS CLI & AWS SDKs

Para ver detalles de una unidad organizativa

Puede utilizar los siguientes comandos para ver detalles de una unidad organizativa:

- AWS CLI,AWSSDK:
  - list-roots

- lista-hijos
- Describe-organizational-unit

El siguiente ejemplo muestra cómo buscar el ID de en unidad organizativa utilizando elAWS CLI. Encontrará el ID de unidad organizativa atravesando la jerarquía comenzando por el parámetro`list-roots`y, a continuación, realizar`list-children`en la raíz e iterativamente en cada uno de sus hijos hasta que encuentre el que desee.

```
$ aws organizations list-roots
{
    "Roots": [
        {
            "Id": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "PolicyTypes": []
        }
    ]
}
$ aws organizations list-children --parent-id r-a1b2 --child-type ORGANIZATIONAL_UNIT
{
    "Children": [
        {
            "Id": "ou-a1b2-f6g7h111",
            "Type": "ORGANIZATIONAL_UNIT"
        }
    ]
}
```

Después de tener el ID de la unidad organizativa, el siguiente ejemplo muestra cómo recuperar los detalles sobre la unidad organizativa.

```
$ aws organizations describe-organizational-unit --organizational-unit-id ou-a1b2-
f6g7h111
{
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h111",
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h111",
        "Name": "Production-Apps"
    }
}
```

- AWSSDK:
  - ListRoots
  - ListChildren
  - DescribeOrganizationalUnit

Consultar detalles de una cuenta

Cuando inicia sesión en la cuenta de administración de la organización en elAWS Organizationsconsole Puede ver los detalles de sus cuentas.

Permisos mínimos

Para ver los detalles de un Cuenta de AWS Debe contar con los siguientes permisos:

- `organizations:DescribeAccount`

- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:ListAccounts`: solo se requiere cuando se utiliza la consola de Organizations

AWS Management Console

Para ver los detalles de un Cuenta de AWS

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. Vaya a la . Cuentas de AWS y elija el nombre del nombre de la cuenta (no el botón de opción) que desea examinar. Si la cuenta que desea es un hijo de una unidad organizativa, es posible que tenga que elegir el icono del triángulo ▶ junto a una unidad organizativa para expandirla y ver a sus hijos. Repite hasta que encuentre la cuenta.

   LaDetalles de la cuentamuestra la información sobre la cuenta.

AWS CLI & AWS SDKs

Para ver los detalles de un Cuenta de AWS

Puede utilizar los siguientes comandos para ver detalles de una cuenta:

- AWS CLI:
  - listas-cuentas— enumera los detalles deTodoCuentas de la organización
  - Describe-account— muestra los detalles de sólo la cuenta especificada

  Ambos comandos devuelven los mismos detalles para cada cuenta incluida en la respuesta.

  El siguiente ejemplo muestra cómo recuperar los detalles de una cuenta especificada.

```
$ aws organizations describe-account --account-id 123456789012

{
    "Account": {
        "Id": "123456789012",
        "Arn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
        "Email": "admin@example.com",
        "Name": "Example.com Organization's Management Account",
        "Status": "ACTIVE",
        "JoinedMethod": "INVITED",
        "JoinedTimestamp": "2020-11-20T09:04:20.346000-08:00"
    }
}
```

- AWSSDK:
  - ListAccounts
  - DescribeAccount

Consultar detalles de una política

Cuando inicia sesión en la cuenta de administración de la organización en elAWS Organizationsconsole Puede ver los detalles de sus políticas.

Permisos mínimos

Para ver los detalles de una política, debe contar con los siguientes permisos:

- `organizations:DescribePolicy`
- `organizations:ListPolicies`

AWS Management Console

Para ver los detalles de una política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. Lleve a cabo una de las siguientes operaciones:
   - Vaya a la .Políticasy, a continuación, elija el tipo de política para la política que desea examinar.
   - Vaya a la . Cuentas de AWS y, a continuación, desplácese hasta una unidad organizativa o cuenta a la que está asociada la política. Por último, elija la opciónPolíticaspara ver la lista de directivas adjuntas.
3. Elija el nombre de la política (no el botón de opción).

   En la páginaDetalles dede la directiva, puede ver toda la información acerca de la directiva, incluido el texto de la directiva JSON, y la lista de unidades organizativas y cuentas a las que está asociada la directiva.

AWS CLI & AWS SDKs

Para ver los detalles de una política

Puede utilizar uno de los siguientes comandos para ver los detalles de una política:

- AWS CLI:
  - list-policies
  - Describe-policy— muestra los detalles de sólo la política especificada

El siguiente ejemplo muestra cómo buscar el identificador de política de la política que desea examinar. Debe especificar un tipo de directiva y el comando devuelve todas las directivas de ese tipo únicamente.

```
$ aws organizations list-policies --filter BACKUP_POLICY
{
    "Policies": [
        {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "test-backup-policy",
            "Description": "test-policy-description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        }
    ]
}
```

La respuesta incluye todos los detalles excepto el documento de política JSON.

En el ejemplo siguiente se muestra cómo recuperar los detalles de sólo la directiva especificada, incluido el documento de directiva JSON.

```
$ aws organizations describe-policy --policy-id p-i9j8k7l6m5
{
    "Policies": [
        {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "test-backup-policy",
            "Description": "test-policy-description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"plans\":{\"My-Backup-Plan\":{\"regions\":{\"@@assign\":[\"us-
west-2\"]},\"rules\":{\"My-Backup-Rule\"
                    :{\"target_backup_vault_name\":{\"@@assign\":\"My-Primary-Backup-
Vault\"}}},\"selections\":{\"tags\":{
                    \"My-Backup-Plan-Resource-Assignment\":{\"iam_role_arn\":
{\"@@assign\":\"arn:aws:iam::$account:role/
                    My-Backup-Role\"},\"tag_key\":{\"@@assign\":\"Stage\"},\"tag_value
\":{\"@@assign\":[\"Production\"]}}}}}}}"
    ]
}
```

- AWSSDK:
  - ListPolicies
  - DescribePolicy

Eliminar la organización mediante la eliminación de la cuenta de administración

Cuando ya no necesite una organización, puede eliminarla. Esto elimina la cuenta de administración de la organización y la propia organización. La antigua cuenta de administración se convierte en una Cuenta de AWS . A continuación, tiene tres opciones: Puede continuar usándola como cuenta independiente, puede utilizarla para crear otra organización o puede aceptar una invitación de otra organización para añadir la cuenta a dicha organización como cuenta miembro.

Important

- Si elimina una organización, no puede recuperarla. Si creó una política dentro de la organización, también se eliminará y no podrá recuperarla.
- Solo puede eliminar una organización después de eliminar todas las cuentas miembro de la organización. Si creó algunas de sus cuentas miembro mediante AWS Organizations, es posible que se le haya bloqueado la eliminación de esas cuentas. Puede eliminar una cuenta miembro solo si esta tiene toda la información necesaria para operar como Cuenta de AWS . Para obtener más información sobre cómo proporcionar dicha información y, a continuación, eliminar la cuenta, consulteAbandonar una organización como cuenta miembro (p. 74).
- Si cerró una cuenta de miembro antes de eliminarla de la organización, ésta ingresará en un estado «suspendido» durante un período de tiempo y no podrá eliminar la cuenta de la organización hasta que finalmente se cierre. Esto puede tardar hasta 90 días y puede impedir que elimine la organización hasta que todas las cuentas miembro estén completamente cerradas.

Cuando se elimina la cuenta de administración de una organización mediante la eliminación de la propia organización, puede afectar a la cuenta de las siguientes formas:

- La cuenta es responsable de pagar únicamente sus propios cargos y ya no es responsable de los cargos generados por cualquier otra cuenta.
- La integración con otros servicios podría estar deshabilitada. Por ejemplo, AWS Single Sign-On requiere una organización para operar, por lo que si elimina una cuenta de una organización que admite AWS SSO, los usuarios de esa cuenta ya no podrán utilizar dicho servicio.

La cuenta de administración de una organización nunca se ve afectada por las políticas de control de servicios (SCP), por lo que no hay ningún cambio en los permisos una vez que las SCP dejan de estar disponibles.

Permisos mínimos

Para eliminar una organización, debe iniciar sesión como usuario o rol de IAM en la cuenta de administración y contar con los siguientes permisos:

- `organizations:DeleteOrganization`
- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations

AWS Management Console

Para eliminar la cuenta de administración de una organización y la propia organización

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. Para poder eliminar la organización, primero debe eliminar todas las cuentas de la organización. Para obtener más información, consulte Eliminación de una cuenta miembro de la organización (p. 71) .
3. Vaya a la .Configuracióny, a continuación, elijaEliminar organización.
4. En el navegadorEliminar organización, introduzca el ID de la organización que se muestra en la línea situada encima del cuadro de texto. A continuación, elijaEliminar organización.
5. (Opcional) Si también desea cerrar la cuenta de administración, puede seguir los pasos que se indican enCierre de un Cuenta de AWS (p. 76).

AWS CLI & AWS SDKs

Para eliminar la cuenta de administración de una organización y la propia organización

Puede utilizar uno de los siguientes comandos para eliminar una organización:

- AWS CLI:Eliminar organización

  En el siguiente ejemplo se elimina la organización para la que se utiliza la propiedad Cuenta de AWS cuyas credenciales se utilizan es la cuenta de administración.

  ```
  $ aws organizations delete-organization
  ```

  Este comando no genera ninguna salida cuando se realiza correctamente.
- AWSSDK: DeleteOrganization

Administración del Cuentas de AWS En su organización

Una organización es una colección de Cuentas de AWS que manejan juntos. Puede realizar las siguientes tareas para administrar las cuentas que forman parte de su organización:

- Consultar los detalles de las cuentas de su organización (p. 48). Puede ver el número de ID único de la cuenta, su Nombre de recurso de Amazon (ARN) y sus políticas asociadas.
- Invitar a Cuentas de AWS Para unirse a su organización (p. 54). Cree invitaciones, administre las invitaciones que ha creado y acepte o rechace invitaciones.
- Creación de un Cuenta de AWS Como parte de su organización (p. 63). Cree y obtenga acceso a un Cuenta de AWS que forma parte automáticamente de su organización.
- Elimine un Cuenta de AWS Desde la organización (p. 71). Como administrador de la cuenta de administración, elimine las cuentas miembro de su organización que ya no desee administrar. Como administrador de una cuenta miembro, elimine la cuenta de su organización. Si la cuenta de administración ha asociado una política a su cuenta miembro, tal vez no pueda eliminar su cuenta.
- Eliminar (o cerrar) un Cuenta de AWS (p. 76). Cuando ya no necesite un Cuenta de AWS , puede cerrar la cuenta para evitar su uso o la acumulación de cargos.

Impacto de estar en una organización

- ¿Qué es? Cuenta de AWS thatCombinaciones¿Una organización? (p. 53)
- ¿Qué es? Cuenta de AWS Que ustedcreate¿En una organización? (p. 54)

Impacto en una Cuenta de AWS que se une a una organización?

Cuando invitas a un Cuenta de AWS Para unirse a una organización, y el propietario de la cuenta acepta la invitación,AWS OrganizationsRealiza automáticamente los siguientes cambios en la cuenta miembro nueva:

- AWS Organizations crea un rol vinculado al servicio denominado `AWSServiceRoleForOrganizations (p. 236)`. La cuenta debe tener este rol si su organización admite todas las características. Puede eliminar el rol si la organización únicamente admite el conjunto de características de facturación unificada. Si elimina la función y posteriormente habilita todas las características en su organización, AWS Organizations vuelve a crear la función para la cuenta.
- Es posible que tenga una variedad de políticas asociadas a la raíz de la organización o a la unidad organizativa que contiene la cuenta. Si es así, dichas políticas se aplican de inmediato a todos los usuarios y roles de la cuenta invitada.
- Puede hacer lo siguientehabilitar la confianza de servicio para otroAWSServicio (p. 237)Para su organización. Tras ello, ese servicio de confianza puede crear roles vinculados a servicios o realizar acciones en cualquier cuenta miembro de la organización, incluida una cuenta invitada.

> Note
>
> Para las cuentas de los miembros invitados,AWS OrganizationsNo crea automáticamente el rol de IAMOrganizationAccountAccessRole (p. 69). Este rol otorga a los usuarios de la cuenta

de administración acceso administrativo a la cuenta de miembro. Si desea habilitar ese nivel de control administrativo en una cuenta invitada, puede añadir manualmente el rol. Para obtener más información, consulte Creación de OrganizationAccountAccessRole en una cuenta miembro invitada (p. 68).

Puede invitar a una cuenta a unirse a una organización que solo tenga habilitadas las características de facturación unificada. Si posteriormente desea habilitar todas las características para la organización, las cuentas invitadas deben aprobar el cambio.

Impacto en una Cuenta de AWS ¿Qué se crea en una organización?

Al crear un Cuenta de AWS En su organización,AWS OrganizationsRealiza automáticamente los siguientes cambios en la cuenta miembro nueva:

- AWS Organizations crea un rol vinculado al servicio denominado `AWSServiceRoleForOrganizations (p. 236)`. La cuenta debe tener este rol si su organización admite todas las características. Puede eliminar el rol si la organización únicamente admite el conjunto de características de facturación unificada. Si elimina la función y posteriormente habilita todas las características en su organización, AWS Organizations vuelve a crear la función para la cuenta.
- AWS Organizationscrea el rol de IAMOrganizationAccountAccessRole (p. 69). Este rol concede a la cuenta de administración acceso a la nueva cuenta miembro. Aunque este papelCANse elimine, le recomendamos que no lo elimine para que esté disponible como opción de recuperación.
- Si tiene algunadirectivas asociadas a la raíz del árbol de la unidad organizativa (p. 86), dichas políticas se aplican inmediatamente a todos los usuarios y roles de la cuenta creada. Las cuentas nuevas se añaden a la OU raíz de forma predeterminada.
- Si tiene habilitada la confianza de servicio para otro servicio de AWS (p. 237) en la organización, ese servicio de confianza puede crear funciones vinculadas a servicios o realizar acciones en cualquier cuenta miembro de la organización, incluida la cuenta creada.

Invitar a Cuenta de AWS Para unirse a su organización

Una vez que haya creado una organización y verificado que es el propietario de la dirección de correo electrónico asociada a la cuenta de administración, puede invitar a Cuentas de AWS para unirse a su organización.

Cuando invita a una cuenta, AWS Organizations envía una invitación al propietario de la cuenta, quien decidirá si desea aceptar o rechazar la invitación. Puede utilizar la consola de AWS Organizations para iniciar y administrar las invitaciones que envíe a otras cuentas. Solo puede enviar una invitación a otra cuenta desde la cuenta de administración de su organización.

Si usted es el administrador de un Cuenta de AWS , también puede aceptar o rechazar una invitación de una organización. Si la acepta, su cuenta se convierte en miembro de esa organización. Su cuenta puede unirse a una única organización, por lo que si recibe varias invitaciones de unión, solo puede aceptar una.

En el momento en que una cuenta acepta la invitación para unirse a una organización, la cuenta de gestión de la organización se hace responsable de todos los cargos acumulados por la nueva cuenta de miembro. El método de pago asociado a la cuenta de miembro ya no se utiliza. En su lugar, el método de pago adjunto a la cuenta de gestión de la organización paga todos los cargos acumulados por la cuenta de miembro.

Cuando una cuenta invitada se une a su organización, no tendrá automáticamente control de administrador pleno sobre la cuenta, a diferencia de las cuentas creadas. Si desea que la cuenta de

administración tenga control administrativo completo sobre una cuenta miembro invitada, debe crear el`OrganizationAccountAccessRole`rol de IAM en la cuenta de miembro y conceder permiso a la cuenta de administración para que asuma el rol. Para configurar esto, una vez que la cuenta invitada se convierta en una cuenta miembro, siga los pasos de Creación de OrganizationAccountAccessRole en una cuenta miembro invitada (p. 68).

> **Note**
>
> Cuando crea una cuenta en su organización en lugar de invitar a una cuenta existente a unirse,AWS Organizationscrea automáticamente un rol de IAM (denominado`OrganizationAccountAccessRole`De forma predeterminada) que puede utilizar para conceder a los usuarios de la cuenta de administración acceso de administrador a la cuenta creada.

AWS Organizations crea automáticamente una función vinculada al servicio en las cuentas miembro invitadas para permitir la integración entre AWS Organizations y otros servicios de AWS. Para obtener más información, consulte AWS Organizations y roles vinculados al servicio (p. 236) .

Para ver el número de invitaciones que puede enviar por día, consulteValores mínimos y máximos (p. 330). Las invitaciones aceptadas no se contabilizan en esta cuota. Tan pronto como se acepta una invitación, puede enviar otra invitación ese mismo día. Todas las invitaciones deben responderse en un plazo de 15 días o caducarán.

Una invitación enviada a una cuenta se contabiliza para la cuota de cuentas de la organización. La cuenta se restaura si la cuenta invitada rechaza la invitación, la cuenta de administración cancela la invitación o la invitación caduca.

Para crear una cuenta que forme parte automáticamente de su organización, consulte Creación de un Cuenta de AWS En su organización (p. 63).

> **Important**
>
> Debido a restricciones legales y de facturación, puede invitar a Cuentas de AWS sólo desde el mismoAWSvendedor yAWScomo la cuenta de administración.

- Todas las cuentas de una organización deben proceder del mismo vendedor registrado que la cuenta de gestión. Si una cuenta proviene deAWSen los Estados Unidos, y otra cuenta proviene de unAWSdistribuidor en la Unión Europea, y otro de unAWSrevendedor en la India, entonces no pueden estar en la misma organización.
- Todas las cuentas de una organización deben proceder del mismoAWScomo la cuenta de administración. Cuentas en el comercial Regiones de AWS no puede estar en una organización con cuentas de la partición Regiones de China o cuentas en elAWSPartición de Regiones GovCloud (US).

Enviar invitaciones a Cuentas de AWS

Para invitar a cuentas a su organización, primero debe verificar que es el propietario de la dirección de correo electrónico asociada a la cuenta de administración. Para obtener más información, consulte Verificación de dirección de correo electrónico (p. 36) . Una vez que haya verificado la dirección de correo electrónico, siga estos pasos para invitar a otras cuentas a que se unan a su organización.

Permisos mínimos

Para invitar a una Cuenta de AWS Para unirse a su organización, debe disponer de los siguientes permisos:

- `organizations:DescribeOrganization` (solo consola)

- `organizations:InviteAccountToOrganization`

AWS Management Console

Para invitar a otra cuenta a que se una a su organización

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. Si ya has verificado tu dirección de correo electrónico conAWS, omita este paso.

   Si aún no ha verificado su dirección de correo electrónico, siga las instrucciones decorreo electrónico de verificación (p. 36)dentro de las 24 horas siguientes a la creación de la organización. Puede pasar algún tiempo hasta que reciba el mensaje de correo electrónico de verificación. No puede invitar a ninguna cuenta a unirse a su organización hasta que haya verificado su dirección de correo electrónico.
3. Vaya a la . Cuentas de AWS y elijaAdición de unAWSaccount.
4. En la páginaAdición de un Cuenta de AWS , elijaInvitar a unaAWSaccount.
5. En la páginaInvitar a unaAWS, paraDirección de correo electrónico o ID de cuenta del Cuenta de AWS Para invitar aIntroduzca la dirección de correo electrónico asociada a la cuenta que se va a invitar o su número de ID de cuenta.
6. (Opcional) ParaMensaje para incluir en el mensaje de correo electrónico de invitación, escriba el texto que desee incluir en la invitación por correo electrónico al propietario de la cuenta invitada.
7. (Opcional) En elAgregue etiquetas, especifique una o más etiquetas que se apliquen automáticamente a la cuenta después de que su administrador acepte la invitación. Para ello, elijaAñada etiquetay, a continuación, introduzca una clave y un valor opcional. Dejar el valor en blanco lo establece en una cadena vacía; no es`null`. Puede asociar hasta 50 etiquetas a una Cuenta de AWS .
8. Seleccione Send invitation (Enviar invitación).

   Important

   Si obtiene un mensaje en el que se indica que ha superado las cuotas de la organización o que no puede agregar una cuenta porque la organización aún se está inicializando, póngase en contacto con AWS Support.
9. La consola le redirige a lainvitationsEn la que puede ver todas las invitaciones abiertas y aceptadas aquí. La invitación que acaba de crear aparece en la parte superior de la lista con el estado establecido en OPEN.

   AWS Organizations envía una invitación a la dirección de correo electrónico del propietario de la cuenta que ha invitado a la organización. Este mensaje de correo electrónico incluye un enlace aAWS Organizations, donde el propietario de la cuenta puede ver los detalles y decidir aceptar o rechazar la invitación. El propietario de la cuenta invitada puede también omitir el mensaje de correo electrónico, ir directamente a laAWS Organizations, ver la invitación y aceptarla o rechazarla.

   La invitación a esta cuenta se contabiliza de inmediato para el número máximo de cuentas que puede tener en su organización. AWS Organizations no espera hasta que la cuenta acepta la invitación. Si la cuenta invitada rechaza la invitación, la cuenta de administración cancela la invitación. Si la cuenta invitada no responde en el periodo de tiempo especificado, la invitación caducará. En cualquier caso, la invitación ya no se contabiliza para la cuota.

AWS CLI & AWS SDKs

Para invitar a otra cuenta a que se una a su organización

Puede utilizar uno de los siguientes comandos para invitar a otra cuenta a unirse a su organización:

- AWS CLI:invite-account-to-organization

```
$ aws organizations invite-account-to-organization \
    --target '{"Type": "EMAIL", "Id": "juan@example.com"}' \
    --notes "This is a request for Juan's account to join Bill's organization."
{
    "Handshake": {
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/invite/
h-examplehandshakeid111",
        "ExpirationTimestamp": 1482952459.257,
        "Id": "h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                 "Type": "ORGANIZATION"
            },
            {
                 "Id": "juan@example.com",
                 "Type": "EMAIL"
            }
        ],
        "RequestedTimestamp": 1481656459.257,
        "Resources": [
            {
                "Resources": [
                    {
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@amazon.com"
                    },
                    {
                         "Type": "MASTER_NAME",
                         "Value": "Management Account"
                    },
                    {
                         "Type": "ORGANIZATION_FEATURE_SET",
                         "Value": "FULL"
                    }
                ],
                "Type": "ORGANIZATION",
                "Value": "o-exampleorgid"
            },
            {
                "Type": "EMAIL",
                "Value": "juan@example.com"
            }
        ],
        "State": "OPEN"
    }
}
```

- AWSSDK de. InviteAccountToOrganization

Administrar las invitaciones pendientes de su organización

Cuando inicie sesión en su cuenta de administración, puede ver todos los Cuentas de AWS En su organización y cancele todas las invitaciones pendientes (abiertas). Para ello, siga los pasos que se describen a continuación.

Permisos mínimos

Para administrar las invitaciones pendientes de su organización, debe contar con los siguientes permisos:

- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:ListHandshakesForOrganization`
- `organizations:CancelHandshake`

AWS Management Console

Para ver o cancelar las invitaciones que se envían desde su organización a otras cuentas

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. Vaya a la .invitations(Se ha creado el certificado).

   Esta página muestra todas las invitaciones que se envían desde su organización y su estado actual.

   > **Note**
   >
   > Las invitaciones aceptadas, canceladas y rechazadas siguen apareciendo en la lista durante 30 días. Posteriormente, se eliminan y ya no aparecen en la lista.

3. Elija el botón de opción Al lado de la invitación que desea cancelar y, a continuación, elijaCancelar invitación. Si el botón de opción está atenuado, entonces esa invitación no se puede cancelar.

   El estado de la invitación cambia deOPENDe aCANCELADO.

   AWSenvía un correo electrónico al propietario de la cuenta para indicarle que ha cancelado la invitación. La cuenta ya no puede unirse a la organización a menos que envíe una nueva invitación.

AWS CLI & AWS SDKs

Para ver o cancelar las invitaciones que se envían desde su organización a otras cuentas

Puede utilizar los siguientes comandos para ver o cancelar invitaciones:

- AWS CLI:List-handshakes-for-organization,Cancelar protocolo de enlace
- En el ejemplo siguiente se muestran las invitaciones enviadas por esta organización a otras cuentas.

```
$ aws organizations list-handshakes-for-organization
{
    "Handshakes": [
        {
            "Action": "INVITE",
            "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
            "ExpirationTimestamp": 1482952459.257,
            "Id": "h-examplehandshakeid111",
            "Parties": [
                {
                    "Id": "o-exampleorgid",
```

```
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "juan@example.com",
                    "Type": "EMAIL"
                }
            ],
            "RequestedTimestamp": 1481656459.257,
            "Resources": [
                {
                    "Resources": [
                        {
                            "Type": "MASTER_EMAIL",
                            "Value": "bill@amazon.com"
                        },
                        {
                            "Type": "MASTER_NAME",
                            "Value": "Management Account"
                        },
                        {
                            "Type": "ORGANIZATION_FEATURE_SET",
                            "Value": "FULL"
                        }
                    ],
                    "Type": "ORGANIZATION",
                    "Value": "o-exampleorgid"
                },
                {
                    "Type": "EMAIL",
                    "Value": "juan@example.com"
                },
                {
                    "Type":"NOTES",
                    "Value":"This is an invitation to Juan's account to join Bill's
 organization."
                }
            ],
            "State": "OPEN"
        },
        {
            "Action": "INVITE",
            "State":"ACCEPTED",
            "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
            "ExpirationTimestamp": 1.471797437427E9,
            "Id": "h-examplehandshakeid222",
            "Parties": [
                {
                    "Id": "o-exampleorgid",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "anika@example.com",
                    "Type": "EMAIL"
                }
            ],
            "RequestedTimestamp": 1.469205437427E9,
            "Resources": [
                {
                    "Resources": [
                        {
                            "Type":"MASTER_EMAIL",
                             "Value":"bill@example.com"
                        },
                        {
                            "Type":"MASTER_NAME",
```

```
                            "Value":"Management Account"
                        }
                    ],
                    "Type":"ORGANIZATION",
                    "Value":"o-exampleorgid"
                },
                {
                    "Type":"EMAIL",
                    "Value":"anika@example.com"
                },
                {
                    "Type":"NOTES",
                    "Value":"This is an invitation to Anika's account to join Bill's
 organization."
                }
            ]
        }
    ]
}
```

En el ejemplo siguiente se muestra cómo cancelar una invitación a una cuenta de.

```
$ aws organizations cancel-handshake --handshake-id h-examplehandshakeid111
{
    "Handshake": {
        "Id": "h-examplehandshakeid111",
        "State":"CANCELED",
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/invite/
h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "susan@example.com",
                "Type": "EMAIL"
            }
        ],
        "Resources": [
            {
                "Type": "ORGANIZATION",
                "Value": "o-exampleorgid",
                "Resources": [
                    {
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@example.com"
                    },
                    {
                        "Type": "MASTER_NAME",
                        "Value": "Management Account"
                    },
                    {
                        "Type": "ORGANIZATION_FEATURE_SET",
                        "Value": "CONSOLIDATED_BILLING"
                    }
                ]
            },
            {
                "Type": "EMAIL",
                "Value": "anika@example.com"
            },
            {
```

```
                "Type": "NOTES",
                "Value": "This is a request for Susan's account to join Bob's
 organization."
            }
        ],
        "RequestedTimestamp": 1.47008383521E9,
        "ExpirationTimestamp": 1.47137983521E9
    }
}
```

- AWSSDK de. ListHandshakesForOrganization,CancelHandshake

Aceptar o rechazar una invitación de una organización

Sus Cuenta de AWS Puede recibir una invitación para unirse a una organización. Puede aceptar o rechazar la invitación. Para ello, siga los pasos que se describen a continuación.

Note

El estado de una cuenta con una organización afecta a los datos de costo y uso visibles:

- Si una cuenta miembro deja una organización y pasa a ser una cuenta independiente, la cuenta ya no tiene acceso a los datos de costo y uso del intervalo de tiempo en el que la cuenta era miembro de la organización. La cuenta tiene acceso únicamente a los datos que se generan como cuenta independiente.
- Si una cuenta miembro deja una organización A para unirse a una organización B, la cuenta ya no tiene acceso a los datos de costo y uso del intervalo de tiempo en el que la cuenta era miembro de la organización A. La cuenta tiene acceso únicamente a los datos que se generan como miembro de la organización B.
- Si una cuenta vuelve a unirse a una organización a la que pertenecía anteriormente, la cuenta vuelve a recuperar el acceso a sus datos históricos de costos y uso.

Permisos mínimos

Para aceptar o rechazar una invitación para unirse a una organización de AWS, debe disponer de los siguientes permisos:

- `organizations:ListHandshakesForAccount`— Necesario para ver la lista de invitaciones en laAWS Organizationsconsola de .
- `organizations:AcceptHandshake`.
- `organizations:DeclineHandshake`.
- `iam:CreateServiceLinkedRole`: necesario solo cuando aceptamos la invitación, requiere crear una función vinculada al servicio en la cuenta miembro para facilitar la integración con otrasAWSServicios de . Para obtener más información, consulte AWS Organizations y roles vinculados al servicio (p. 236) .

AWS Management Console

Para aceptar o rechazar una invitación

1. Una invitación para unirse a una organización se envía a la dirección de correo electrónico del propietario de la cuenta. Si es el propietario de la cuenta y recibe un mensaje de correo electrónico de invitación, siga las instrucciones indicadas en el correo electrónico de invitación o vaya aAWS Organizationsconsoleen el navegador y, a continuación, elijainvitations, o vaya directamente a laInvitación de la cuenta de miembro(Se ha creado el certificado).

2. Si se le pide, inicie sesión en la cuenta invitada como usuario de IAM, asuma una función de IAM o inicie sesión como usuario raíz de la cuenta (No recomendado).
3. LaInvitación de la cuenta de miembromuestra las invitaciones abiertas de su cuenta para unirse a organizaciones.

   SeleccionarAceptar invitaciónorDeclinationsegún proceda.

   - Si eligeAceptar invitaciónEn el paso anterior, la consola le redirige a laInformación general acerca deCon detalles de la organización de la que su cuenta ahora es miembro. Puede ver el ID de organización y la dirección de correo electrónico del propietario.

     Note

     Las invitaciones aceptadas siguen apareciendo en la lista durante 30 días. Posteriormente, se eliminan y ya no aparecen en la lista.

     AWS Organizations crea automáticamente una función vinculada al servicio en la nueva cuenta miembro para permitir la integración entre AWS Organizations y otros servicios de AWS. Para obtener más información, consulte AWS Organizations y roles vinculados al servicio (p. 236) .

     AWSenvía un correo electrónico al propietario de la cuenta de administración de la organización para indicarle que ha aceptado la invitación. También envía un correo electrónico al propietario de la cuenta miembro para indicarle que la cuenta ahora es miembro de la organización.
   - Si eligeDeclinationEn el paso anterior, la cuenta permanece en laInvitación de la cuenta de miembroque enumera cualquier otra invitación pendiente.

     AWSenvía un correo electrónico al propietario de la cuenta de administración de la organización para indicarle que ha rechazado la invitación.

     Note

     Las invitaciones rechazadas siguen apareciendo en la lista durante 30 días. Posteriormente, se eliminan y ya no aparecen en la lista.

AWS CLI & AWS SDKs

Para aceptar o rechazar una invitación

Puede utilizar los siguientes comandos para aceptar o rechazar invitaciones:

- AWS CLI:Aceptar un apretón de manos,Cómo declinar un apretón de manos

  En el ejemplo siguiente se muestra cómo aceptar una invitación para unirse a una organización.

```
$ aws organizations accept-handshake --handshake-id h-examplehandshakeid111
{
    "Handshake": {
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/invite/
h-examplehandshakeid111",
        "RequestedTimestamp": 1481656459.257,
        "ExpirationTimestamp": 1482952459.257,
        "Id": "h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "juan@example.com",
                "Type": "EMAIL"
```

```
            }
        ],
        "Resources": [
            {
                "Resources": [
                    {
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@amazon.com"
                    },
                    {
                        "Type": "MASTER_NAME",
                        "Value": "Management Account"
                    },
                    {
                        "Type": "ORGANIZATION_FEATURE_SET",
                         "Value": "ALL"
                    }
                ],
                "Type": "ORGANIZATION",
                "Value": "o-exampleorgid"
            },
            {
                "Type": "EMAIL",
                "Value": "juan@example.com"
            }
        ],
        "State": "ACCEPTED"
    }
}
```

En el ejemplo siguiente se muestra cómo rechazar una invitación para unirse a una organización.

- AWSSDK de. AcceptHandshake,DeclineHandshake

Creación de un Cuenta de AWS En su organización

En esta página se describe cómo crear cuentas dentro de su organización en AWS Organizations. Para obtener información acerca de cómo empezar a trabajar conAWSy creando un solo Cuenta de AWS , consulte laCentro de recursos introductorios.

Una organización es una colección de Cuentas de AWS que gestiona de forma centralizada. Puede realizar los siguientes procedimientos para administrar las cuentas que forman parte de su organización:

- Creación de un Cuenta de AWS Que forme parte de su organización (p. 64)
- Acceso a una cuenta miembro con un rol de acceso a la cuenta de administración (p. 69)

Important

- Cuando crea una cuenta miembro en su organizaciónAWS Organizationscrea automáticamenteAWS Identity and Access Management(IAM) en la cuenta miembro. Este rol permite a los usuarios de IAM de la cuenta de administración que asuman el rol ejercer control administrativo completo sobre la cuenta miembro. Esta función está sujeta a las políticas de control de servicios (SCP) (p. 108) que se aplican a la cuenta miembro.

  AWS Organizations también crea automáticamente una función vinculada al servicio denominada `AWSServiceRoleForOrganizations`, que permite la integración con determinados servicios de AWS. Debe configurar los demás servicios para permitir la integración. Para obtener más información, consulte AWS Organizations y roles vinculados al servicio (p. 236) .

- Si esta organización se administra conAWS Control Towery, a continuación, cree sus cuentas mediante elAWS Control Toweren laAWS Control Towerconsola o API. Si creas una cuenta en Organizations, esa cuenta no está inscrita enAWS Control Tower. Para obtener más información, consulteReferencia a recursos fuera deAWS Control Toweren laAWS Control TowerGuía del usuario de.

Note

Cuentas de AWS que cree como parte de una organización no se suscriben automáticamente aAWSLos correos electrónicos de marketing Para suscribir sus cuentas para recibir correos electrónicos de marketing, consultehttps://pages.awscloud.com/communication-preferences.

Creación de un Cuenta de AWS Que forme parte de su organización

Cuando inicia sesión en la cuenta de administración de la organización, puede crear cuentas de miembros de que se conviertan automáticamente en cuentas de su organización. Para ello, siga los pasos que se describen a continuación.

Al crear una cuenta utilizando el siguiente procedimiento, las Organizations copian automáticamente la siguiente información de la cuenta de administración a la nueva cuenta miembro:

- Nombre de cuenta
- Número de teléfono
- Nombre de la empresa
- URL del cliente
- Email
- Idioma de comunicación
- Marketplace (proveedor de la cuenta en algunos Regiones de AWS)

AWS does noRecopilar automáticamente toda la información necesaria para que una cuenta opere como cuenta independiente. Si alguna vez necesita eliminar la cuenta de la organización y convertirla en cuenta independiente, debe proporcionar dicha información para la cuenta antes de poder eliminarla. Para obtener más información, consulte Abandonar una organización como cuenta miembro (p. 74) .

Permisos mínimos

Para crear una cuenta miembro en su organización, debe contar con los permisos siguientes:

- `organizations:CreateAccount`
- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
- `iam:CreateServiceLinkedRole` (concedido a la entidad principal `organizations.amazonaws.com` para permitir la creación del rol vinculado al servicio requerido en las cuentas miembro).

AWS Management Console

Para crear un Cuenta de AWS Que forme parte automáticamente

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.

2. En la página Cuentas de AWS ElijaAdición de un Cuenta de AWS .
3. En la páginaAdición de un Cuenta de AWS ElijaCreación de un Cuenta de AWS (Se elige de forma predeterminada)
4. En la páginaCreación de un Cuenta de AWS page, for Cuenta de AWS Nombre deIntroduzca el nombre que desea asignar a la cuenta. Este nombre le ayuda a distinguir más adelante la cuenta de todas las demás cuentas de la organización y es independiente del alias de IAM o del nombre de correo electrónico del propietario.
5. ParaDirección de correo electrónico del propietario de la cuenta, escriba la dirección de correo electrónico del propietario de la cuenta. Esta dirección de correo electrónico ya no se puede asociar a otra Cuenta de AWS porque se convierte en la credencial de nombre de usuario para el usuario raíz de la cuenta.
6. (Opcional) Especifique el nombre que va a asignar al rol de IAM que se crea automáticamente en la nueva cuenta. Este rol concede a la cuenta de administración de la organización permiso para tener acceso a la cuenta miembro que acaba de crear. Si no especifica un nombre, AWS Organizations asigna a la función el nombre predeterminado de `OrganizationAccountAccessRole`. Recomendamos que utilice el nombre predeterminado en todas las cuentas para lograr coherencia.

   Important

   Recuerde este nombre de rol. Lo necesitará más adelante para conceder acceso a la nueva cuenta a los usuarios de IAM de la cuenta de administración.
7. (Opcional) En elAgregue etiquetas, agregue una o más etiquetas a la nueva cuentaAgregue etiquetaA continuación, introduzca una clave y un valor opcional. Dejar el valor en blanco lo establece en una cadena vacía; no es`null`. Puede asociar hasta 50 etiquetas a una cuenta.
8. Seleccione Create (Crear) Cuenta de AWS .

   - Si aparece un error que indica que ha superado la cuota de cuenta de la organización, consulteObtengo un mensaje de "cuota superada" cuando intento agregar una cuenta a mi organización (p. 336).
   - Si obtiene un error que indica que no puede añadir una cuenta porque la organización todavía se está inicializando, espere una hora y vuelva a intentarlo.
   - También puede comprobar el registro de AWS CloudTrail para obtener información acerca de si la creación de la cuenta se ha realizado correctamente. Para obtener más información, consulte Registro y monitoreo en AWS Organizations (p. 321) .
   - Si el error persiste, póngase en contacto con AWS Support.

   La Cuentas de AWS Aparece, con su nueva cuenta agregada a la lista.
9. Ahora que ya ha creado la cuenta y tiene un rol de IAM que concede acceso de administrador a los usuarios de la cuenta de administración, puede tener acceso a la cuenta siguiendo los pasos deAcceso y administración de las cuentas miembro de la organización (p. 66).

   Note

   Cuando crea una cuentaAWS OrganizationsAl principio asigna una contraseña larga (64 caracteres), compleja y generada aleatoriamente al usuario raíz. No puede recuperar esta contraseña inicial. Para obtener acceso a la cuenta como usuario raíz por primera vez, debe seguir el proceso de recuperación de contraseña. Para obtener más información, consulte Acceso a una cuenta miembro como usuario raíz (p. 67) .

AWS CLI & AWS SDKs

Para crear un Cuenta de AWS Que forme parte automáticamente

Puede utilizar uno de los siguientes comandos para crear una cuenta:

- AWS CLI:Create account (Crear cuenta)

```
$ aws organizations create-account \
    --email susan@example.com \
    --account-name "Production Account"
{
        "CreateAccountStatus": {
                "State": "IN_PROGRESS",
                "Id": "car-examplecreateaccountrequestid111"
        }
}
```

A continuación, puede comprobar el estado de la creación de la cuenta con el siguiente comando.

```
$ aws organizations describe-create-account-status \
    --create-account-request-id car-examplecreateaccountrequestid111
{
  "CreateAccountStatus": {
    "State": "SUCCEEDED",
    "AccountId": "555555555555",
    "AccountName": "Production account",
    "RequestedTimestamp": 1470684478.687,
    "CompletedTimestamp": 1470684532.472,
    "Id": "car-examplecreateaccountrequestid111"
  }
}
```

- AWSSDK CreateAccount

Acceso y administración de las cuentas miembro de la organización

Cuando crea una cuenta de en su organización,Además del usuario raíz,AWS Organizationscrea automáticamente un rol de IAM que de forma predeterminada se denomina`OrganizationAccountAccessRole`. Puede especificar un nombre diferente al crearlo; sin embargo, le recomendamos que le asigne un nombre coherente en todas sus cuentas. En esta guía, haremos referencia al rol por el nombre predeterminado.AWS OrganizationsNo crea ningún otro usuario, grupo u otras funciones de IAM. Para tener acceso a las cuentas de su organización, debe utilizar uno de los siguientes métodos:

- La cuenta tiene un usuario raíz que puede utilizar para iniciar sesión. Le recomendamos que utilice únicamente el usuario raíz para crear usuarios, grupos y roles de IAM y que siempre inicie sesión con una de estas entidades. Consulte Acceso a una cuenta miembro como usuario raíz (p. 67).
- Si crea una cuenta utilizando las herramientas proporcionadas como parte deAWS Organizations, puede acceder a la cuenta mediante el rol preconfigurado denominado`OrganizationAccountAccessRole`que existe en todas las cuentas nuevas que cree de esta manera. Consulte Acceso a una cuenta miembro con un rol de acceso a la cuenta de administración (p. 69).
- Si invita a una cuenta existente a que se una a su organización y la cuenta acepta la invitación, puede elegir crear una función de IAM que permita a la cuenta de administración tener acceso a la cuenta de miembro invitada. Se pretende que este rol sea idéntico al rol que se añade automáticamente a una cuenta que se crea con AWS Organizations. Para crear esta función, consulte Creación de OrganizationAccountAccessRole en una cuenta miembro invitada (p. 68). Después de crear la función, puede tener acceso a él siguiendo los pasos de Acceso a una cuenta miembro con un rol de acceso a la cuenta de administración (p. 69).

- Utilice AWS Single Sign-On y habilite el acceso de confianza para AWS SSO con AWS Organizations. Esto permite a los usuarios iniciar sesión enAWS SSOCon sus credenciales corporativas y acceder a recursos en su cuenta de administración asignada o en sus cuentas miembro.

  Para obtener más información, consulteAdministrar el SSO a su Cuentas de AWS en laAWS Single Sign-OnGuía del usuario de . Para obtener más información acerca de cómo configurar el acceso de confianza para AWS SSO, consulte AWS Single Sign-On y AWS Organizations (p. 298).

  #### Permisos mínimos

  Para obtener acceso a Cuenta de AWS De cualquier otra cuenta de su organización, debe contar con el permiso siguiente:

  - `sts:AssumeRole`— El`Resource`: el elemento debe estar establecido en un asterisco (*) o en el ID de la cuenta con el número de la cuenta con la que el usuario necesita obtener acceso a la nueva cuenta miembro.

Acceso a una cuenta miembro como usuario raíz

Al crear una nueva cuenta, AWS Organizations asigna inicialmente al usuario raíz una contraseña con un mínimo de 64 caracteres. Todos los caracteres se generan de forma aleatoria sin garantías en cuanto al aspecto de determinados conjuntos de caracteres. No puede recuperar esta contraseña inicial. Para obtener acceso a la cuenta como usuario raíz por primera vez, debe seguir el proceso de recuperación de contraseña.

Notes

- Como práctica recomendada, recomendamos que no utilice el usuario raíz para obtener acceso a su cuenta excepto para crear otros usuarios y funciones con permisos más limitados. A continuación, inicie sesión como uno de los usuarios o roles.
- También le recomendamos que establezca la autenticación multifactor (MFA) en el usuario raíz. Restablezca la contraseña y asigne un dispositivo MFA al usuario raíz.
- Si ha creado una cuenta de miembro en una organización con una dirección de correo electrónico incorrecta, no podrá iniciar sesión en la cuenta como usuario raíz. Contact (Contacto)AWSFacturación y SupportPara obtener ayuda.

Console

Para solicitar una nueva contraseña para el usuario raíz de la cuenta miembro

1. Vaya a laInicie sesiónPágina de laAWSconsola de enhttps://console.aws.amazon.com/. Si ya ha iniciado sesión en AWS, debe cerrarla para poder ver la página de inicio de sesión.
2. Si la página Sign in (Iniciar sesión) muestra tres cuadros de texto para Account ID or alias (ID de cuenta o alias), IAM user name (Nombre de usuario de IAM) y Password (Contraseña), entonces elija Sign-in using root account credentials (Iniciar sesión mediante credenciales de cuenta raíz).
3. Escriba la dirección de correo electrónico que está asociada a su Cuenta de AWS Haga clic en y luego enSiguiente.
4. Seleccione Forgot your password? (¿Ha olvidado su contraseña?) y después escriba la información necesaria para crear una contraseña nueva. Para ello, debe poder obtener acceso al correo electrónico entrante enviado a la dirección de correo electrónico asociada a la cuenta.

Creación de OrganizationAccountAccessRole en una cuenta miembro invitada

De forma predeterminada, si crea una cuenta miembro como parte de su organización,AWSCrea automáticamente un rol de en la cuenta que concede permisos de administrador a los usuarios de IAM en la cuenta de administración que puedan asumir el rol. De forma predeterminada, este rol se denomina `OrganizationAccountAccessRole`. Para obtener más información, consulte Acceso a una cuenta miembro con un rol de acceso a la cuenta de administración (p. 69).

Sin embargo, a las cuentas miembro a las que invite a unirse a su organización no se les crea automáticamente un rol de administrador. Tiene que hacerlo manualmente, tal y como se muestra en el siguiente procedimiento. Lo que este procedimiento hace básicamente es duplicar el rol configurado de forma automática para las cuentas creadas. Le recomendamos que utilice el mismo nombre, `OrganizationAccountAccessRole`, para los roles creados manualmente en aras de la coherencia y para que sea fácil de recordar.

Console

Para crear unAWS Organizationsrol de administrador de en una cuenta miembro

1. Inicie sesión en la consola de IAM en https://console.aws.amazon.com/iam/. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) de la cuenta miembro. El usuario o el rol deben tener permiso para crear roles y políticas de IAM.
2. En la consola de IAM, vaya aRoles deHaga clic en y luego enCreación de un rol.
3. SeleccionarOtro Cuenta de AWS .
4. Escriba el número de ID de la cuenta de 12 dígitos de la cuenta de administración a la que desea conceder acceso de administrador y elijaSiguiente: Permisos.

   Para este rol, dado que las cuentas son internas a su empresa, debenoelijaRequire external ID. Para obtener más información acerca de la opción de ID externo, consulte¿Cuándo debería usar el ID externo?en laGuía del usuario de IAM.
5. Si ha habilitado y configurado MFA, puede elegir que se requiera autenticación mediante un dispositivo MFA. Para obtener más información acerca de MFA, consulteUso de Multi-Factor Authentication (MFA) enAWSen laGuía del usuario de IAM.
6. En la páginaAdjuntar directivas de permisosHaga clic en la páginaAWSPolítica administrada`AdministratorAccess`Haga clic en y luego enSiguiente: Tags (Etiquetas).
7. En la páginaAgregar etiquetas (opcional)Haga clic en la páginaSiguiente: Consulte.
8. En la página Review, especifique un nombre del rol y una descripción opcional. Le recomendamos que utilice `OrganizationAccountAccessRole` para mantener la coherencia con el nombre predeterminado asignado al rol en las cuentas nuevas. Para confirmar los cambios, elija Crear rol.
9. Su nuevo rol aparecerá en la lista de roles disponibles. Seleccione el nombre del nuevo rol para ver sus detalles y preste especial atención a la URL de enlace facilitada. Entregue esta URL a los usuarios de la cuenta miembro que necesitan tener acceso al rol. Además, anote el Role ARN (ARN de rol), ya que lo necesitará en el paso 15.
10. Inicie sesión en la consola de IAM en https://console.aws.amazon.com/iam/. Esta vez, inicie sesión como usuario de la cuenta de administración con permisos para crear políticas y asignarlas a los usuarios o grupos.
11. Seleccione Policies (Políticas) y, a continuación, seleccione Create Policy (Crear política).
12. En Service, seleccione STS.
13. En Actions (Acciones), comience a escribir **`AssumeRole`** en el cuadro Filter (Filtro) y marque la casilla cuando aparezca.

14. Seleccione Resources (Recursos), asegúrese de que Specific (Específico) esté seleccionado y seleccione Add ARN (Agregar ARN).
15. Introduzca elAWSEscriba su número de ID de cuenta miembro de y, a continuación, el nombre del rol que haya creado anteriormente en los pasos 1 —8. Elija Add (Agregar).
16. Si está concediendo un permiso para asumir la función en varias cuentas miembro, repita los pasos 14 y 15 para cada cuenta.
17. Elija Review policy (Revisar política).
18. Escriba un nombre para la nueva política y, a continuación, seleccione Create policy (Crear política) para guardar los cambios.
19. Elija Groups (Grupos) en el panel de navegación y, a continuación, elija el nombre del grupo (no la casilla) que desea utilizar para delegar la administración de la cuenta miembro.
20. Elija la pestaña Permissions.
21. SeleccionarAsociar políticaHaga clic en, seleccione la política que creó en los pasos 11 al 18 y, a continuación, elijaAsociar política.

Los usuarios que sean miembros del grupo seleccionado ahora pueden utilizar las direcciones URL que anotó en el paso 9 para obtener acceso al rol de cada cuenta miembro. Pueden obtener acceso a estas cuentas miembro de la misma forma que lo harían si tuvieran acceso a una cuenta que usted haya creado en la organización. Para obtener más información sobre el uso del rol para administrar una cuenta miembro, consulte Acceso a una cuenta miembro con un rol de acceso a la cuenta de administración (p. 69).

Acceso a una cuenta miembro con un rol de acceso a la cuenta de administración

Cuando crea una cuenta miembro con laAWS Organizationsconsola de,AWS Organizations automáticamentecrea un rol de IAM denominado`OrganizationAccountAccessRole`de la cuenta. Este rol tiene permisos administrativos completos en la cuenta miembro. El rol también está configurado para conceder acceso a la cuenta de administración de la organización. Puede crear un rol idéntico para una cuenta miembro invitada siguiendo los pasos que se indican en Creación de OrganizationAccountAccessRole en una cuenta miembro invitada (p. 68). Para utilizar este rol para tener acceso a la cuenta miembro, debe iniciar sesión como usuario de la cuenta de administración que tiene permisos para asumir el rol. Para configurar estos permisos, siga este procedimiento. Le recomendamos que conceda permisos a los grupos en lugar de a los usuarios para simplificar el mantenimiento.

Console

Para conceder permisos a los miembros de un grupo de IAM en la cuenta de administración para tener acceso al rol

1. Inicie sesión en la consola de IAM enhttps://console.aws.amazon.com/iam/como usuario con permisos de administrador en la cuenta de administración. Esto es necesario para delegar permisos al grupo de IAM cuyos usuarios vayan a tener acceso al rol en la cuenta miembro.
2. Comience creando la política administrada que necesitará más tarde en Step 11 (p. 70).

   En el panel de navegación, elija Policies (Políticas) y, a continuación, seleccione Create policy (Crear política).
3. En la pestaña Editor visual, elija Elegir un servicio, escriba **`STS`** en el cuadro de búsqueda para filtrar la lista y, a continuación, elija la opción STS.
4. En la sección Acciones, escriba **`assume`** en el cuadro de búsqueda para filtrar la lista y, a continuación, elija la opción AssumeRole.

5. En la sección de recursos, elija Específico, elija Agregar ARN para restringir el acceso y, a continuación, escriba el número de cuenta de miembro y el nombre del rol que creó en la sección anterior (se recomienda asignarle el nombre `OrganizationAccountAccessRole`).
6. Elija Agregar cuando el cuadro de diálogo muestre el ARN correcto.
7. (Opcional) Si desea requerir Multi-Factor Authentication (MFA) o restringir el acceso al rol desde un intervalo de direcciones IP especificado, expanda la sección Condiciones de solicitud y seleccione las opciones que desee aplicar.
8. Elija Review policy (Revisar política).
9. En el campo Nombre escriba un nombre para la política. Por ejemplo: **`GrantAccessToOrganizationAccountAccessRole`**. También puede añadir una descripción opcional.
10. Elija Crear política para guardar la nueva política administrada.
11. Ahora que tiene la política disponible, puede asociarla a un grupo.

    En el panel de navegación, elija Groups (Grupos) y, a continuación, elija el nombre del grupo (no la casilla) cuyos miembros desea que asuman el rol en la cuenta miembro. Si es necesario, puede crear un grupo nuevo.
12. Elija la pestaña Permisos y, a continuación, en Políticas administradas, elija Asociar política.
13. (Opcional) En el cuadro Buscar puede comenzar a escribir el nombre de la política para filtrar la lista hasta que pueda ver el nombre de la política que acaba de crear en Step 2 (p. 69) mediante Step 10 (p. 70). También puede filtrar todas las políticas administradas de AWS eligiendo Tipo de política y, a continuación, eligiendo Administrada por cliente.
14. Marque la casilla situada junto a la política y, a continuación, elija Asociar política.

Los usuarios de IAM que sean miembros del grupo ahora tendrán permisos para cambiar al nuevo rol en la funciónAWS Organizationsmediante el procedimiento siguiente.

Console

Para cambiar a la función de la cuenta miembro

Cuando se utilice el rol, el usuario tendrá permisos de administrador en la nueva cuenta miembro. Indique a los usuarios de IAM que sean miembros del grupo que hagan lo siguiente para cambiar al nuevo rol.

1. Desde la esquina superior derecha de laAWS Organizations, elija el enlace que contiene el nombre de inicio de sesión y, a continuación, elijaRole de conmutación.
2. Escriba el número de identificación de la cuenta y el nombre de la función proporcionados por el administrador.
3. En Display Name (Nombre de visualización), escriba el texto que desee mostrar en la barra de navegación en la esquina superior derecha en lugar de su nombre de usuario mientras utiliza la función. Si lo desea, puede elegir un color.
4. Elija Switch Role. Ahora, todas las acciones que realice se harán con los permisos concedidos a la función a la que ha cambiado. Ya no tendrá los permisos asociados a su usuario de IAM de original hasta que cambie otra vez a esta función.
5. Cuando haya terminado de realizar acciones que requieran los permisos del rol, puede volver a su usuario de IAM normal. Elija el nombre de la función en la esquina superior derecha, independientemente de lo que haya especificado como Display Name (Nombre de visualización). A continuación, elija Back to ***`UserName`*** (Volver a UserName).

Recursos adicionales

- Para obtener más información acerca de cómo conceder permisos para cambiar de rol, consulteConceder permisos de usuario para cambiar de rolen laGuía del usuario de IAM.
- Para obtener más información sobre el uso de un rol respecto del que se le hayan concedido permisos para poder asumirlo, consulteCambio a un rol (AWS Management Console)en laGuía del usuario de IAM.
- Para ver un tutorial acerca del uso de las funciones para el acceso entre cuentas, consulteTutorial: Delegar el acceso entre Cuentas de AWS Uso de las funciones de IAMen laGuía del usuario de IAM.
- Para obtener más información sobre el cierre Cuentas de AWS , consulteCierre de un Cuenta de AWS (p. 76).

Eliminación de una cuenta miembro de la organización

Parte de la administración de cuentas en una organización consiste en eliminar las cuentas de miembro que ya no necesita. En esta página se describe lo que debe saber antes de eliminar una cuenta y se indican los procedimientos para eliminar cuentas.

Para obtener información sobre cómo eliminarcuenta de administración, consulteEliminar la organización mediante la eliminación de la cuenta de administración (p. 51).

Temas

Antes de eliminar una cuenta de una organización

Antes de eliminar una cuenta, es importante saber lo siguiente:

- Puede eliminar una cuenta de la organización solo si la cuenta tiene la información que necesita para funcionar como cuenta independiente. Cuando se crea una cuenta en una organización con la consola, la API o los comandos de la AWS Organizations de AWS CLI, toda la información necesaria para las cuentas independientes no se recopila automáticamente. Para cada cuenta que desee convertir en independiente, deberá elegir un plan de soporte, proporcionar y verificar la información de contacto necesaria y proporcionar un método de pago actual.AWSutiliza el método de pago para cargar cualquier factura (noAWSCapa gratuita de)AWSque se produce mientras la cuenta no esté adjunta a una organización.
- Para eliminar una cuenta que creó en la organización, debe esperar al menos siete días después de que se creó la cuenta. Las cuentas invitadas no están sujetas a este período de espera.
- En el momento en que la cuenta abandona con éxito la organización, el propietario de la Cuenta de AWS se hace responsable de todas las nuevasAWSlos costos acumulados, y se utiliza el método de pago de la cuenta. La cuenta de gestión de la organización ya no es responsable.
- La cuenta que desea eliminar no debe ser una cuenta de administrador delegada para cualquierAWShabilitado para su organización. Si la cuenta es un administrador delegado, primero debe cambiar la cuenta de administrador delegada a otra cuenta que quede en la organización. Para obtener más información acerca de cómo desactivar o cambiar la cuenta de administrador delegado para unaAWS, consulte la documentación correspondiente a dicho servicio
- Incluso después de la eliminación de las cuentas creadas (cuentas creadas con elAWS Organizationso la consola`CreateAccount`API) desde dentro de una organización, (i) las cuentas creadas se

rigen por los términos del acuerdo con nosotros de la cuenta de gestión que las haya creado, y (ii) la cuenta de gestión que las haya creado sigue siendo conjunta y solidariamente responsable de las acciones realizadas por sus cuentas creadas. Los acuerdos de los clientes con nosotros y los derechos y obligaciones que implican dichos acuerdos no se pueden asignar ni transferir sin nuestro consentimiento previo. Para obtener nuestro consentimiento, póngase en contacto con nosotros en https://aws.amazon.com/contact-us/.

- Si una cuenta miembro deja una organización, esa cuenta ya no tiene acceso a los datos de costo y uso del intervalo de tiempo en el que la cuenta era miembro de la organización. Sin embargo, la cuenta de administración de la organización puede seguir obteniendo acceso a los datos. Si la cuenta se vuelve a unir a la organización, la cuenta puede obtener de nuevo acceso a esos datos.
- Cuando una cuenta de miembro abandona una organización, se eliminan todas las etiquetas asociadas a la cuenta.

Efectos de la eliminación de una cuenta de una organización

Al eliminar una cuenta de una organización, no se realiza ningún cambio directo en la cuenta. Sin embargo, se producen los siguientes efectos indirectos:

- La cuenta ahora es responsable de pagar sus propios cargos y debe tener asociado un método de pago válido.
- Los principales de la cuenta ya no se verán afectados por ningúnPolíticas de (p. 86)que se aplica en la organización. Esto significa que las restricciones impuestas por SCP ya no existen, y que los usuarios y los roles de la cuenta podrían tener más permisos que antes. Otros tipos de directivas de organización ya no se pueden aplicar ni procesar.
- Si utiliza el`aws:PrincipalOrgID`en cualquier directiva para restringir el acceso solo a usuarios y roles de Cuentas de AWS en su organización, debe revisar y posiblemente actualizar estas directivas antes de eliminar la cuenta de miembro. Si no actualiza las directivas, los usuarios y los roles de la cuenta podrían perder el acceso a los recursos cuando la cuenta abandone la organización.
- La integración con otros servicios podría estar deshabilitada. Si elimina una cuenta de una organización que tiene integración con unAWS, los usuarios de esa cuenta ya no podrán utilizar dicho servicio.

Eliminación de una cuenta miembro de la organización

Cuando inicia sesión en la cuenta de administración de la organización, puede quitar las cuentas miembro de la organización que ya no necesite. Para ello, complete el procedimiento siguiente. Estos procedimientos se aplican únicamente a las cuentas miembro. Para eliminar la cuenta de administración, debeeliminar la organización (p. 51).

> Note
>
> Si una cuenta miembro se elimina de una organización, dicha cuenta miembro ya no estará cubierta por los acuerdos de la organización. Los administradores de cuentas de administración deben comunicar esto a las cuentas miembro antes de eliminar las cuentas miembro de la organización, para que dichas cuentas miembro puedan formalizar nuevos acuerdos si es necesario. Puede consultar una lista de los acuerdos activos de la organización en laAWS Artifacten la consolaAWS Artifactacuerdos de la organización(Se ha creado el certificado).

Permisos mínimos

Para eliminar una o varias cuentas miembro de la organización, debe iniciar sesión como usuario o rol de IAM en la cuenta de administración con los siguientes permisos:

- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:RemoveAccountFromOrganization`

Si decide iniciar sesión como un usuario o un rol de IAM en una cuenta miembro en el paso 6, ese usuario o rol debe tener los siguientes permisos:

- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola Organizations.
- `organizations:LeaveOrganization`: tenga en cuenta que el administrador de la organización puede aplicar una política a la cuenta que elimine este permiso, lo que le impedirá eliminar la cuenta de la organización.
- Si inicia sesión como un usuario de IAM y la cuenta tiene pendiente la información de pago, el usuario de IAM debe tener los permisos`aws-portal:ModifyBillingyaws-portal:ModifyPaymentMethods`. Además, la cuenta miembro debe tener habilitado el acceso del usuario de IAM a la facturación. Si esto no está ya habilitado, consulteActivación del acceso a la consola de Billing and Cost Managementen laAWS Billing and Cost ManagementGuía del usuario de.

AWS Management Console

Para eliminar una cuenta miembro de su organización

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la página Cuentas de AWS , busque y seleccione la casilla de verificación junto a cada cuenta miembro que quiera eliminar de su organización. Puede navegar por la jerarquía de unidades organizativas o habilitarVista Cuentas de AWS Solopara ver una lista plana de cuentas sin la estructura de unidad organizativa. Si tiene muchas cuentas, puede que tenga que elegirCargar más cuentas en 'ou-name'En la parte inferior de la lista para encontrar todas las personas que quiera mover.

   En la página Cuentas de AWS , busque y elija el nombre de la cuenta miembro que desea eliminar de su organización. Es posible que tenga que expandir las unidades organizativas (elija la opción) para encontrar la cuenta que desea.
3. SeleccionarActionsy, a continuación, en Cuenta de AWS , elijaEliminación de la organización.
4. En el navegadorEliminación de la cuenta 'El nombre de la cuenta'(#account-id) de la organización?, elijaRemove account.
5. Si AWS Organizations no consigue eliminar una o más de las cuentas, normalmente se debe a que no ha proporcionado toda la información necesaria para que la cuenta funcione como cuenta independiente. Siga estos pasos:

   a. Inicie sesión en las cuentas con errores. Le recomendamos que inicie sesión en la cuenta miembro seleccionando Copy link y, a continuación, pegándolo en la barra de direcciones en una nueva ventana del navegador de incógnito. Si no utiliza una ventana de incógnito, se cerrará la sesión de la cuenta de administración y no podrá navegar para volver a este cuadro de diálogo.

   b. El navegador le lleva directamente al proceso de registro para completar los pasos que falten para esta cuenta. Complete todos los pasos indicados. Esto podría incluir lo siguiente:

      - Proporcionar información de contacto
      - Proporcionar un método de pago válido
      - Verificar el número de teléfono
      - Seleccionar una opción de plan de soporte

   c. Al completar el último paso del registro, AWS redirige automáticamente su navegador a la consola de AWS Organizations de la cuenta miembro. Seleccione Leave organization y confirme su selección en el cuadro de diálogo de confirmación. Se le redirigirá a la

página Introducción de la consola de AWS Organizations, donde podrá ver las invitaciones pendientes de su cuenta para unirse a otras organizaciones.

AWS CLI & AWS SDKs

Para eliminar una cuenta miembro de su organización

Puede utilizar uno de los siguientes comandos para quitar una cuenta de miembro:

- AWS CLI:Remove-account-from-organization

```
$ aws organizations remove-account-from-organization \
    --account-id 123456789012
```

Este comando no genera ninguna salida cuando se realiza correctamente.

- AWSSDK: RemoveAccountFromOrganization

Abandonar una organización como cuenta miembro

Cuando inicia sesión en una cuenta miembro, puede eliminar esa cuenta de su organización. Para ello, complete el procedimiento siguiente. La cuenta de administración no puede abandonar la organización mediante esta técnica. Para eliminar la cuenta de administración, debeeliminar la organización.

La cuenta que desea eliminar no debe ser una cuenta de administrador delegada para cualquierAWShabilitado para su organización. Si la cuenta es un administrador delegado, primero debe cambiar la cuenta de administrador delegada a otra cuenta que quede en la organización. Para obtener más información acerca de cómo desactivar o cambiar la cuenta de administrador delegado para unaAWS, consulte la documentación correspondiente a dicho servicio

Important

Si abandona una organización, ya no estará cubierto por los acuerdos de la organización que la cuenta de administración de la organización aceptó en su nombre. Puede consultar una lista de estos acuerdos de la organización en laAWS Artifacten la consolaAWS Artifactacuerdos de la organización(Se ha creado el certificado). Antes de abandonar la organización, debe determinar (con la ayuda de los equipos jurídicos, de privacidad o de conformidad, si procede) si es necesario formalizar nuevos acuerdos.

Note

El estado de una cuenta con una organización afecta a los datos de costo y uso visibles:

- Si una cuenta miembro deja una organización y pasa a ser una cuenta independiente, la cuenta ya no tiene acceso a los datos de costo y uso del intervalo de tiempo en el que la cuenta era miembro de la organización. La cuenta tiene acceso únicamente a los datos que se generan como cuenta independiente.
- Si una cuenta miembro deja una organización A para unirse a una organización B, la cuenta ya no tiene acceso a los datos de costo y uso del intervalo de tiempo en el que la cuenta era miembro de la organización A. La cuenta tiene acceso únicamente a los datos que se generan como miembro de la organización B.
- Si una cuenta vuelve a unirse a una organización a la que pertenecía anteriormente, la cuenta vuelve a recuperar el acceso a sus datos históricos de costos y uso.

Permisos mínimos

Para abandonar una organización de AWS, debe disponer de los siguientes permisos:

- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola Organizations.
- `organizations:LeaveOrganization`: tenga en cuenta que el administrador de la organización puede aplicar una política a la cuenta que elimine este permiso, lo que le impedirá eliminar la cuenta de la organización.
- Si inicia sesión como un usuario de IAM y la cuenta tiene pendiente la información de pago, el usuario de IAM debe tener los permisos`aws-portal:ModifyBilling`y`aws-portal:ModifyPaymentMethods`. Además, la cuenta miembro debe tener habilitado el acceso del usuario de IAM a la facturación. Si esto no está ya habilitado, consulteActivación del acceso a la consola de Billing and Cost Managementen laAWS Billing and Cost ManagementGuía del usuario de.

AWS Management Console

Para abandonar una organización como cuenta miembro

1. Inicie sesión enAWS Organizationsen AWS Organizationsconsole. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en una cuenta miembro.

   De forma predeterminada, no tiene acceso a la contraseña de usuario raíz en una cuenta miembro que se haya creado utilizando AWS Organizations. En caso necesario, recupere la contraseña de usuario raíz siguiendo los pasos en Acceso a una cuenta miembro como usuario raíz (p. 67).
2. En la páginaPanel de Organizations, elijaAbandonar organización.
3. Lleve a cabo uno de los siguientes pasos:

   - Si su cuenta tiene toda la información necesaria para operar como una cuenta independiente, aparecerá un cuadro de diálogo de confirmación. Confirme su elección para eliminar la cuenta. Se le redirigirá a la página Introducción de la consola de AWS Organizations, donde podrá ver las invitaciones pendientes de su cuenta para unirse a otras organizaciones.
   - Si su cuenta no tiene toda la información necesaria, realice los pasos siguientes:
     a. Aparecerá un cuadro de diálogo que explica que debe completar algunos pasos adicionales. Haga clic en el enlace.
     b. Complete todos los pasos de inicio de sesión que se indiquen. Esto podría incluir lo siguiente:
        - Proporcionar información de contacto
        - Proporcionar un método de pago válido
        - Verificar el número de teléfono
        - Seleccionar una opción de plan de soporte
     c. Cuando vea el cuadro de diálogo que le avisa de que el proceso de inscripción se ha completado, seleccione Leave organization.
     d. Aparece un cuadro de diálogo de confirmación. Confirme su elección para eliminar la cuenta. Se le redirigirá a la página Introducción de la consola de AWS Organizations, donde podrá ver las invitaciones pendientes de su cuenta para unirse a otras organizaciones.
4. Elimine de la organización los roles de IAM que conceden acceso a su cuenta.

   Important

   Si la cuenta se creó en la organización, las Organizations creadas automáticamente un rol de IAM en la cuenta que habilitó el acceso de la cuenta de administración de la organización. Si la cuenta fue invitada a unirse, las Organizations no crearon automáticamente dicho rol, pero usted u otro administrador podría haber creado uno para obtener los mismos beneficios. En cualquier caso, cuando quita la cuenta de

la organización, dicho rol no se elimina automáticamente. Si desea terminar este acceso desde la cuenta de administración de la organización anterior, debe eliminar manualmente este rol de IAM. Para obtener información sobre cómo eliminar un rol, consulteEliminación de roles o perfiles de instanciaen laIAM User Guide.

AWS CLI & AWS SDKs

Para abandonar una organización como cuenta miembro

Puede utilizar uno de los siguientes comandos para abandonar una organización:

- AWS CLI:Abandonar la organización

  El siguiente ejemplo hace que la cuenta cuyas credenciales se utilizan para ejecutar el comando salga de la organización.

  ```
  $ aws organizations leave-organization
  ```

  Este comando no genera ninguna salida cuando se realiza correctamente.
- AWSSDK: LeaveOrganization

Cierre de un Cuenta de AWS

Este tema se aplica aonly Cuentas de AWS que son administrados por elAWS OrganizationsServicio

- Si desea cerrar uncuenta de Amazon.com, consultehttp://www.amazon.com/gp/help/customer/display.html?nodeId=GDK92DNLSGWTV6MP.
- Si desea cerrar un servicio de Amazon Web Services (AWS) que no forma parte de unaAWSOrganización, consultehttps://aws.amazon.com/premiumsupport/knowledge-center/close-aws-account/.

Si ya no necesita una cuenta de miembro de la organización y desea asegurarse de que nadie incurra en gastos para esa cuenta, puede cerrar la cuenta.

Antes de cerrar la cuenta, realice un seguimiento de las aplicaciones y los datos que desea conservar y elimine el resto deAWSde AWS. Todos los recursos y datos almacenados que hubiera en la cuenta se pierden y no pueden recuperarse. Para obtener más información, consulte el artículo de KB "How do I close my Amazon Web Services account?"

A partir de este momento, la cuenta ya no puede utilizarse para ninguna actividad de AWS aparte de iniciar sesión como usuario raíz para ver las facturas anteriores o ponerse en contacto con AWS Support. Para obtener más información, consulte Cómo ponerse en contacto con el servicio de atención al cliente en referencia a su factura.

Important

- Las cuentas cerradas por 90 días o más ya no son elegibles para su reincorporación. En este punto, los recursos que se encontraban en la cuenta no se pueden recuperar.
- Las cuentas cerradas están visibles su organización con el estado "suspendido". Una vez que una cuenta ha estado suspendida durante 90 días, ya no está visible en su organización.
- Las cuentas solo se pueden cerrar desde la consola Administración de costos y facturación, no desde la consola AWS Organizations ni de sus herramientas.

- Para cerrar la cuenta de administración de la organización, primero debequitar (p. 72)o cierre todas las cuentas miembro de la organización. Esto se debe a que al cerrar la cuenta de administración se elimina automáticamente la organización, que sólo se realiza correctamente si no hay cuentas de miembro en la organización.

Las cuentas solo se pueden cerrar desde la consola Administración de costos y facturación, no desde la consola AWS Organizations ni de sus herramientas.

Para cerrar una cuenta de administración, primero debeeliminar la organización (p. 51)A continuación, puede cerrarla siguiendo los pasos del siguiente procedimiento.

Console

Para cerrar un Cuenta de AWS

Recomendado Antes de cerrar la cuenta, realice un seguimiento de las aplicaciones y los datos que desea conservar y elimine el resto deAWSde AWS.AWSno puede recuperar ni restaurar los recursos ni los datos de la cuenta después de cerrarla.

1. Inicie sesión como usuario raíz de la cuenta que desea cerrar, utilizando la dirección de correo electrónico y la contraseña asociados a la cuenta. Si inicia sesión como un usuario o una función de IAM, no puede cerrar cuentas.

   Note

   De forma predeterminada, las cuentas miembro que crea con AWS Organizations no tienen una contraseña asociada al usuario raíz de la cuenta. Para iniciar sesión, debe solicitar una contraseña para el usuario raíz. Para obtener más información, consulte Acceso a una cuenta miembro como usuario raíz (p. 67).
2. Abra el iconoBilling and Cost Management de.
3. En la barra de navegación situada en la esquina superior derecha, elija su nombre de cuenta (o alias) y, a continuación, elija Mi cuenta.
4. En la página Configuración de cuenta, desplácese hasta el final de la página a la sección Cerrar cuenta. Lea el texto situado junto a la casilla de verificación y asegúrese de que lo entiende.
5. Seleccione la casilla de verificación para confirmar que entiende las condiciones y, a continuación, elija Cerrar cuenta.
6. En el cuadro de confirmación, elija Cerrar cuenta.

Después de cerrar un Cuenta de AWS , ya no puede usarla para obtener acceso aAWSservicios o recursos. Durante los 90 días siguientes al cierre de su cuenta (el "Periodo posterior al cierre"), podrá iniciar sesión para ver las facturas anteriores y obtener acceso a AWS Support. Puede ponerse en contacto con AWS Support dentro del Periodo posterior al cierre para reabrir la cuenta. Para obtener más información, consulteCómo vuelvo a abrir el Cuenta de AWS ?en el Knowledge Center.

Note

Por razones de seguridad,AWS nuncavuelve a utilizar un Cuenta de AWS Número de ID después de cerrar la cuenta. Como resultado de esta medida de seguridad, si deja un ID de una cuenta cerrada en una política de IAM, nunca podría haber una cuenta desconocida con el mismo ID que tendría acceso a sus recursos. Sin embargo, le recomendamos que elimine las referencias a cuentas cerradas, de acuerdo con la práctica recomendada de seguridad de conceder el mínimo privilegio necesario para realizar el trabajo.

Administración de unidades organizativas

Puede utilizar unidades organizativas para agrupar las cuentas que desee administrar como una sola unidad. Esto simplifica enormemente la administración de sus cuentas. Por ejemplo, puede asociar un control basado en políticas a una unidad organizativa para que todas las cuentas de la unidad organizativa hereden automáticamente la política. Puede crear varias unidades organizativas dentro de una única organización, y puede crear unidades organizativas dentro de otras unidades organizativas. Cada unidad organizativa puede contener varias cuentas, y puede mover cuentas de una unidad organizativa a otra. Sin embargo, los nombres de las unidades organizativas deben ser únicos dentro de una unidad organizativa o nodo raíz.

> **Note**
>
> Hay una raíz en la organización, queAWS Organizationscrea cuando usted configura por primera vez su organización.

Para estructurar las cuentas de su organización, puede realizar las siguientes tareas:

- Consultar los detalles de una unidad organizativa (p. 47)
- Crear una unidad organizativa (p. 79)
- Cambiar el nombre de una unidad organizativa (p. 81)
- Editar etiquetas asociadas a una unidad organizativa (p. 82)
- Mover una cuenta a una unidad organizativa o entre el nodo raíz y las unidades organizativas (p. 83)

Navegar por el nodo raíz y la jerarquía de la unidad organizativa

Para navegar por distintas unidades organizativas o al nodo raíz al desplazar cuentas o adjuntar políticas, puede utilizar la vista predeterminada «árbol».

AWS Management Console

Para navegar por la organización como un 'árbol'

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la página Cuentas de AWS , al principio de la páginaOrganización, asegúrese de que elVista Cuentas de AWS Soloel icono de cambio está giradoDESACAR.  .
3. En un principio, aparece el árbol mostrando la raíz, mostrando sólo el primer nivel de unidades organizativas secundarias y cuentas. Para ampliar el árbol para mostrar niveles más profundos, elija el icono de ampliar (▶) junto a cualquier entidad padre. Para reducir el desorden y contraer una rama del árbol, elija el icono de contraer (▼) junto a una entidad padre expandida.
4. Elija el nombre de una unidad organizativa o raíz para ver sus detalles y realizar determinadas operaciones. Como alternativa, puede elegir el botón de opción situado junto al nombre y realizar ciertas operaciones en esa entidad en el cuadroActionsMenú de.

También puede ver la lista de solo las cuentas de su organización en forma tabular, sin tener que desplazarse primero a una unidad organizativa para encontrarlas. En esta vista, no puede ver ninguna de las unidades organizativas ni manipular las directivas adjuntas a ellas.

AWS Management Console

Para ver la organización como una lista plana de cuentas sin jerarquía

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la página Cuentas de AWS , al principio de la páginaOrganización, elija la opciónVista Cuentas de AWS Solopara activarlo.  .
3. La lista de cuentas se muestra sin ninguna jerarquía.

Crear una unidad organizativa

Cuando inicia sesión en la cuenta de administración de su organización, puede crear una unidad organizativa en el nodo raíz de su organización. Las unidades organizativas se pueden anidar hasta un máximo de cinco niveles de profundidad. Para crear una unidad organizativa, siga los pasos que se describen a continuación.

Important

Si esta organización se administra conAWS Control Towery, a continuación, cree sus unidades organizativas con elAWS Control Towerconsola o API. Si crea la unidad organizativa en Organizations, esa unidad organizativa no está registrada conAWS Control Tower. Para obtener más información, consulteReferencia a recursos fuera deAWS Control Toweren laAWS Control TowerGuía del usuario de.

Permisos mínimos

Para crear una unidad organizativa dentro de un nodo raíz de su organización, debe contar con los permisos siguientes:

- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:CreateOrganizationalUnit`

AWS Management Console

Para crear una unidad organizativa (OU)

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. Vaya a la página Cuentas de AWS .

   La consola muestra la unidad organizativa raíz y su contenido. La primera vez que visite el nodo raíz, la consola mostrará todas las Cuentas de AWS en esa vista de nivel superior. Si previamente ha creado unidades organizativas y ha movido cuentas a ellas, la consola muestra únicamente las unidades organizativas de nivel superior y todas las cuentas que aún no ha movido a una unidad organizativa.
3. (Opcional) Si desea crear una unidad organizativa dentro de otra existente,navegar a la unidad organizativa secundaria (p. 78)Elija el nombre (no la casilla) de la unidad organizativa

secundaria, o elija la opción ▶ junto a las unidades organizativas en la vista de árbol hasta que vea la que desea y, a continuación, elija su nombre.

4. Cuando haya seleccionado la unidad organizativa principal correcta en la jerarquía, en la pestañaActionsmenú, enOrganizational Unit, elijaCrear nuevos
5. En el navegadorCrear unidad organizativaEn el cuadro de diálogo, escriba el nombre de la unidad organizativa que desea crear.
6. (Opcional) Agregue una o varias etiquetas eligiendoAñada etiquetaY después ingresando una clave y un valor opcional. Dejar el valor en blanco lo establece en una cadena vacía; no es`null`. Puede asociar hasta 50 etiquetas a una unidad organizativa.
7. Por último, elijaCrear unidad organizativa.

La nueva unidad organizativa aparecerá dentro de la principal. Ahora puede mover cuentas a esta unidad organizativa (p. 83) o asociarle políticas.

AWS CLI & AWS SDKs

Para crear una unidad organizativa (OU)

Puede utilizar uno de los siguientes comandos para crear una unidad organizativa:

- AWS CLI:Crear unidad organizativa

  Para crear una unidad organizativa, primero debe buscar la identidad de la raíz o unidad organizativa que desea que sea la principal de la nueva unidad organizativa.

  Para encontrar la identidad de la raíz, utilice ellist-rootscomando. Para encontrar la identidad de una unidad organizativa, utilice la herramientalista-hijospara navegar a la unidad organizativa que desee.

  En el ejemplo siguiente se muestra cómo buscar la identidad de la raíz y, a continuación, buscar la identidad de una unidad organizativa bajo la raíz. El último comando muestra cómo crear una nueva unidad organizativa en la unidad organizativa encontrada.

```
$ aws organizations list-roots
{
    "Roots": [
        {
            "Id": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "PolicyTypes": []
        }
    ]
}
$ aws organizations list-children \
    --parent-id r-a1b2 \
    --child-type ORGANIZATIONAL_UNIT
{
    "Children": [
        {
            "Id": "ou-a1b2-f6g7h111",
            "Type": "ORGANIZATIONAL_UNIT"
        }
    ]
}
$ aws organizations create-organizational-unit \
    --parent-id ou-a1b2-f6g7h111 \
    --name New-Child-OU
{
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h222",
```

```
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
        "Name": "New-Child-OU"
    }
}
```

- AWSSDK: CreateOrganizationalUnit

Cambiar el nombre de una unidad organizativa

Cuando inicia sesión en la cuenta de administración de su organización, puede cambiar el nombre de una unidad organizativa. Para ello, siga los pasos que se describen a continuación.

Permisos mínimos

Para cambiar el nombre de una unidad organizativa dentro de un nodo raíz de su organización de AWS, debe contar con los permisos siguientes:

- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:UpdateOrganizationalUnit`

AWS Management Console

Para cambiar el nombre de una unidad organizativa

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la página Cuentas de AWS Página,navegar a la unidad organizativa (p. 78)Para cambiar el nombre y, a continuación, lleve a cabo alguno de los siguientes pasos:
   - Elija el botón de opciónJunto a la unidad organizativa cuyo nombre desea cambiar. A continuación, en elActionsmenú, enunidad organizativa, elijaCambio de nombre.
   - Elija el nombre de la unidad organizativa para acceder a la página de detalles de la unidad organizativa. A continuación, en la parte superior de la página elijaCambio de nombre.
3. En el navegadorCambiar el nombre de unidad organizativaEn el cuadro de diálogo, escriba un nuevo nombre y, a continuación, elijaGuarde los cambios.

AWS CLI & AWS SDKs

Para cambiar el nombre de una unidad organizativa

Puede utilizar uno de los siguientes comandos para cambiar el nombre de una unidad organizativa:

- AWS CLI:update-organizational-unit

  En el siguiente ejemplo se muestra cómo cambiar el nombre de una unidad organizativa.

```
$ aws organizations update-organizational-unit \
    --organizational-unit-id ou-a1b2-f6g7h222 \
    --name "Renamed-OU"
{
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h222",
```

```
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
        "Name": "Renamed-OU"
    }
}
```

- AWSSDK: UpdateOrganizationalUnit

Edición de etiquetas asociadas a una unidad organizativa

Cuando inicia sesión en la cuenta maestra de su organización, puede agregar o quitar las etiquetas asociadas a una unidad organizativa. Para ello, siga los pasos que se describen a continuación.

Permisos mínimos

Para editar las etiquetas asociadas a una unidad organizativa dentro de un nodo raíz en el nodoAWSEn la organización, debe contar con los siguientes permisos:

- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:DescribeOrganizationalUnit`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

Para editar las etiquetas asociadas a una unidad organizativa

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la página Cuentas de AWS Página,Desplácese y elija el nombre de la unidad organizativa (p. 78)cuyas etiquetas desea editar.
3. En la página de detalles de la unidad organizativa, elija el botónEtiquetasy después elija.Administrar etiquetas.
4. Puede realizar cualquiera de estas acciones en esta pestaña:
   - Edite el valor de cualquier etiqueta introduciendo un nuevo valor sobre el anterior. No se puede modificar la clave de etiqueta. Para cambiar una clave, debe eliminar la etiqueta con la clave anterior y agregar una etiqueta con la nueva clave.
   - Elimine una etiqueta existente seleccionandoRemoveJunto a la etiqueta que desea remive.
   - Añada una clave de etiqueta y un par de valor nuevo. SeleccionarAñada etiquetay, a continuación, introduzca el nuevo nombre de clave y el valor opcional en los cuadros proporcionados. Si deja elValorEn el cuadro vacío, el valor es una cadena vacía;`null`.
5. SeleccionarGuarde los cambiosdespués de haber realizado todas las adiciones, eliminaciones y ediciones que desee realizar.

AWS CLI & AWS SDKs

Para editar las etiquetas asociadas a una unidad organizativa

Puede utilizar uno de los siguientes comandos para cambiar las etiquetas asociadas a una unidad organizativa:

- AWS CLI:tag-resourceyuntag-resource

  En el siguiente ejemplo se asocia la etiqueta`"Department"="12345"`A una unidad organizativa. Tenga en cuenta que`Key`y`Value`Distinguen entre mayúsculas

```
$ aws organizations tag-resource \
    --resource-id ou-a1b2-f6g7h222 \
    --tags Key=Department,Value=12345
```

  Este comando no genera ninguna salida cuando se realiza correctamente.

  En el ejemplo siguiente se quita el`Department`desde una unidad organizativa.

```
$ aws organizations untag-resource \
    --resource-id ou-a1b2-f6g7h222 \
    --tag-keys Department
```

  Este comando no genera ninguna salida cuando se realiza correctamente.
- AWSSDK: TagResourceyUntagResource

Mover cuentas a una unidad organizativa o entre el nodo raíz y las unidades organizativas

Cuando inicia sesión en la cuenta de administración de su organización, puede mover las cuentas de su organización desde el raíz a una unidad organizativa, de una unidad organizativa a otra, o de vuelta al raíz desde una unidad organizativa. Al colocar una cuenta dentro de una unidad organizativa, esta obtiene todas las políticas que se han asociado a la unidad organizativa principal y a todas las unidades organizativas que van desde la principal hasta el nodo raíz. Si una cuenta no está en una unidad organizativa, solo tendrá las políticas que se han asociado directamente al objeto raíz y las políticas que se han asociado directamente a la cuenta. Para mover cuentas, lleve a cabo los siguientes pasos.

Permisos mínimos

Para mover cuentas a una nueva ubicación en la jerarquía de unidades organizativas, debe contar con los permisos siguientes:

- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:MoveAccount`

AWS Management Console

Para mover cuentas a una unidad organizativa

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la página Cuentas de AWS En la página, busque la cuenta o cuentas que desea mover. Puede navegar por la jerarquía de unidades organizativas o habilitarVista Cuentas de AWS Solopara ver una lista plana de cuentas sin la estructura de unidad organizativa. Si tiene muchas cuentas,

puede que tenga que elegirCargar más cuentas en 'Nombre de OU'En la parte inferior de la lista para encontrar todas las que desea mover.

3. Elija la casilla de verificación Junto al nombre de cada cuenta que desea mover.
4. En la páginaActionsmenú, en Cuenta de AWS , elijaMover.
5. En el navegadorMover Cuenta de AWS En el cuadro de diálogo, vaya a y, a continuación, elija la unidad organizativa o el nodo raíz al que desea mover la cuenta y, a continuación, elijaMover Cuenta de AWS .

AWS CLI & AWS SDKs

Para mover una cuenta a una unidad organizativa

Puede utilizar uno de los siguientes comandos para mover una cuenta:

- AWS CLI:move-account

  En el ejemplo siguiente se mueve un Cuenta de AWS de la raíz a una unidad organizativa. Tenga en cuenta que debe especificar los ID de los contenedores de origen y de destino.

```
$ aws organizations move-account \
    --account-id 111122223333 \
    --source-parent-id r-a1b2 \
    --destination-parent-id ou-a1b2-f6g7h111
```

  Este comando no genera ninguna salida cuando se realiza correctamente.
- AWSSDK: MoveAccount

Eliminación de unidades organizativas

Cuando inicia sesión en la cuenta de administración de su organización, puede eliminar todas las unidades organizativas que ya no necesite.

En primer lugar, debe mover todas las cuentas fuera de la unidad organizativa y de todas las unidades organizativas secundarias, y después eliminar las unidades organizativas secundarias.

Permisos mínimos

Para eliminar una unidad organizativa, debe contar con los permisos siguientes:

- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:DeleteOrganizationalUnit`

AWS Management Console

Para eliminar una unidad organizativa

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la página Cuentas de AWS En la página, busque las unidades organizativas que desea eliminar y seleccione la casilla de verificación. junto al nombre de cada unidad organizativa.
3. SeleccionarActionsy después enunidad organizativa, elijaEliminar.

4. Para confirmar que desea eliminar las unidades organizativas, introduzca el nombre de la unidad organizativa (si eligió eliminar sólo una) o la palabra «eliminar» (si eligió más de una) y, a continuación, elijaEliminar.

   AWS Organizationselimina las unidades organizativas y las quita de la lista.

AWS CLI & AWS SDKs

Para eliminar una unidad organizativa

Puede utilizar uno de los siguientes comandos para eliminar una unidad organizativa:

- AWS CLI:Eliminar unidad organizativa

  En el siguiente ejemplo se muestra cómo eliminar una unidad organizativa.

```
$ aws organizations delete-organizational-unit \
    --organizational-unit-id ou-a1b2-f6g7h222
```

  Este comando no genera ninguna salida cuando se realiza correctamente.
- AWSSDK: DeleteOrganizationalUnit

Administración de políticas de AWS Organizations

Políticas deAWS Organizationsle permiten aplicar tipos adicionales de administración a Cuentas de AWS en su organización, Puede utilizar políticas cuando todas las características están habilitadas (p. 37) en su organización.

La consola de AWS Organizations muestra los tipos de políticas que están habilitados o deshabilitados. En la pestaña Organize accounts (Organizar cuentas), elija `Root` en el panel de navegación izquierdo. El panel de detalles del lado derecho de la pantalla muestra todos los tipos de políticas disponibles. La lista indica cuáles están habilitados y cuáles están deshabilitados en la raíz de esa organización. Si está disponible la opción Enable (Habilitar) para un tipo, significa que ese tipo está deshabilitado actualmente. Si está disponible la opción Disable (Deshabilitar) para un tipo, significa que ese tipo está habilitado actualmente.

Tipos de políticas

Las Organizations ofrecen tipos de políticas en las dos categorías generales siguientes:

Políticas de autorización

Las políticas de autorización le ayudan a administrar de forma centralizada la seguridad de Cuentas de AWS en su organización,

- Las políticas de control de servicios (SCP) (p. 108) ofrecen un control central sobre los máximos permisos disponibles para todas las cuentas de su organización.

Políticas de administración

Las políticas de administración le permiten configurar y administrar de forma centralizada los servicios de AWS y sus características.

- Políticas de exclusión de servicios de inteligencia artificial (IA) (p. 144)le permiten controlar la recopilación de datos paraAWSServicios de IA para todas las cuentas de su organización.
- Las políticas de copia de seguridad (p. 160) le ayudan a administrar y aplicar planes de copias de seguridad a los recursos de AWS de las cuentas de su organización de manera centralizada.
- Las políticas de etiquetado (p. 195) le ayudan a estandarizar las etiquetas asociadas a los recursos de AWS de las cuentas de su organización.

En la tabla siguiente se resumen algunas de las características de cada tipo de política:

Tipo de política	Afecta a la cuenta	Número máximo que se puede asociar a una raíz, unidad organizativa o cuenta	Tamaño máximo	Admite la visualización de directivas efectivas para la unidad organizativa o
SCP	No	5	5120 bytes	No
Política de exclusión de servicios de IA	Sí	5	2500 caracteres	Sí
Política Backup de	Sí	10	10,000 caracteres	Sí
Política de etiquetas	Sí	5	2500 caracteres	Sí

Uso de políticas en su organización

Habilitar y deshabilitar tipos de política

Para habilitar un tipo de política

Antes de poder crear y adjuntar una política a su organización, debe habilitar ese tipo de políticas para su uso. Habilitar un tipo de política es una tarea única en la raíz de la organización. Solo puede habilitar un tipo de política desde la cuenta de administración de la organización.

Permisos mínimos

Para habilitar un tipo de política, necesita permiso para ejecutar las siguientes acciones:

- `organizations:EnablePolicyType`
- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola Organizations
- `organizations:ListRoots`: solo se requiere cuando se utiliza la consola Organizations

AWS Management Console

Para habilitar un tipo de política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaPolíticas, elija el nombre del tipo de política que desea habilitar.
3. En la página de tipo de directiva, elijaHabilitar***Tipo de política***.

   La página se sustituye por una lista de las directivas disponibles del tipo especificado.

AWS CLI & AWS SDKs

Para habilitar un tipo de política

Puede utilizar uno de los comandos siguientes para habilitar un tipo de política:

- AWS CLI:Habilitación de tipo política

  En el siguiente ejemplo, se muestra cómo habilitar políticas de copia de seguridad para la organización. Tenga en cuenta que debe especificar el ID de la raíz de su organización.

```
$ aws organizations enable-policy-type \
    --root-id r-a1b2 \
    --policy-type BACKUP_POLICY
{
    "Root": {
        "Id": "r-a1b2",
        "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
        "Name": "Root",
        "PolicyTypes": [
            {
                "Type": "BACKUP_POLICY",
                "Status": "ENABLED"
            }
        ]
    }
}
```

  Lista de`PolicyTypes`en la salida ahora incluye el tipo de directiva especificado con el parámetro`Status`de`ENABLED`.
- AWSSDK: EnablePolicyType

Deshabilitar un tipo de política

Si ya no desea utilizar un tipo de política determinado en su organización, puede deshabilitarlo para evitar su uso accidental. Solo puede deshabilitar un tipo de política desde la cuenta de administración de la organización.

Important

- Cuando deshabilita un tipo de política, todas las políticas del tipo especificado se separan automáticamente de todas las entidades de la raíz de la organización. Las políticas no se eliminan.
- (Solo para el tipo de política de control de servicios) Si vuelve a habilitar el tipo de política SCP más adelante, inicialmente todas las entidades de la raíz de la organización se adjuntan solo

al`FullAWSAccess`SCP Los archivos adjuntos de SCPs a entidades se pierden cuando los SCP están deshabilitados en la organización. Si posteriormente desea volver a habilitar SCP, debe volver a adjuntarlos a la raíz, las unidades organizativas y las cuentas de la organización, según corresponda.

Permisos mínimos

Para deshabilitar las SCP, necesita permiso para ejecutar las siguientes acciones:

- `organizations:DisablePolicyType`
- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola Organizations
- `organizations:ListRoots`: solo se requiere cuando se utiliza la consola Organizations

AWS Management Console

Para deshabilitar un tipo de política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaPolíticas, elija el nombre del tipo de política que desea deshabilitar.
3. En la página de tipo de directiva, elijaDeshabilitar***Tipo de política***.
4. En el cuadro de diálogo de confirmación, escriba la palabra**disable**A continuación, elijaDeshabilitar.

   La lista de directivas disponibles del tipo especificado desaparece.

AWS CLI & AWS SDKs

Para deshabilitar un tipo de política

Puede utilizar uno de los comandos siguientes para deshabilitar un tipo de política:

- AWS CLI:Deshabilitar el tipo de política

  En el siguiente ejemplo, se muestra cómo deshabilitar políticas de copia de seguridad para la organización. Tenga en cuenta que debe especificar el ID de la raíz de su organización.

```
$ aws organizations disable-policy-type \
    --root-id r-a1b2 \
    --policy-type BACKUP_POLICY
{
    "Root": {
        "Id": "r-a1b2",
        "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
        "Name": "Root",
        "PolicyTypes": []
    }
}
```

  Lista de`PolicyTypes`en la salida ya no incluye el tipo de directiva especificado.

- AWSSDK: DisablePolicyType

Obtener información sobre las políticas de su organización

En esta sección se describen varias maneras de obtener información acerca de las políticas de la organización. Estos procedimientos se aplican a todos los tipos de políticas. Debe habilitar un tipo de política en la raíz de la organización antes de poder asociar políticas de ese tipo a cualquier entidad en la raíz de esa organización.

Enumeración de todas las políticas

Permisos mínimos

Para mostrar las políticas de su organización, debe contar con el permiso siguiente:

- `organizations:ListPolicies`

Puede ver las directivas de su organización en elAWS Management Consoleo mediante unAWS Command Line Interface(AWS CLI) o un comandoAWSOperación SDK.

AWS Management Console

Para enumerar todas las políticas de una organización

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaPolíticas, elija el tipo de política que desee mostrar.

   Si el tipo de directiva especificado está habilitado, la consola muestra una lista de todas las directivas de ese tipo que están disponibles actualmente en la organización.
3. Vuelva a la seccióny repita para cada tipo de directiva.

AWS CLI & AWS SDKs

Para enumerar todas las políticas de una organización

Puede utilizar uno de los siguientes comandos para enumerar las políticas de una organización:

- AWS CLI: list-policies

  En el siguiente ejemplo se muestra cómo obtener una lista de todas las políticas de control de servicios de la organización. Debe especificar el tipo de directiva que desea ver. Repita el comando para cada tipo de política que desee incluir.

```
$ aws organizations list-policies \
    --filter SERVICE_CONTROL_POLICY
{
    "Policies": [
        {
            "Id": "p-FullAWSAccess",
            "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-
FullAWSAccess",
            "Name": "FullAWSAccess",
            "Description": "Allows access to every operation",
            "Type": "SERVICE_CONTROL_POLICY",
```

```
            "AwsManaged": true
        }
    ]
}
```

- AWSSDK: ListPolicies

Mostrar las políticas asociadas a un nodos raíz, unidad organizativa o cuenta

Permisos mínimos

Para mostrar las políticas que están asociadas a un nodos raíz, unidad organizativa o cuenta de la organización, debe contar con el permiso siguiente:

- `organizations:ListPoliciesForTarget`con un`Resource`en la misma declaración de política que incluye el nombre de recurso de Amazon (ARN) del destino especificado (o «*»)

AWS Management Console

Para enumerar todas las políticas que están asociadas directamente a un nodos raíz, unidad organizativa o cuenta específica

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la página Cuentas de AWS , elija el nombre de la raíz, unidad organizativa o cuenta cuyas políticas desea ver. Es posible que tenga que expandir las unidades organizativas (elija la opción ▶) para encontrar la OU que desea.
3. En la página raíz, unidad organizativa o cuenta, elija la opciónPolíticasPestaña.

   LaPolíticasmuestra todas las políticas asociadas a esa raíz, unidad organizativa o cuenta, agrupadas por tipo de política.

AWS CLI & AWS SDKs

Para enumerar todas las políticas que están asociadas directamente a un nodos raíz, unidad organizativa o cuenta específica

Puede utilizar uno de los siguientes comandos para enumerar las políticas que están adjuntas a una entidad:

- AWS CLI:list-policies-for-target

  En el ejemplo siguiente se enumeran todas las directivas de control de servicio asociadas a la unidad organizativa especificada. Debe especificar tanto el ID de la raíz, la unidad organizativa o la cuenta como el tipo de directiva que desea enumerar.

```
$ aws organizations list-policies-for-target \
    --target-id ou-a1b2-f6g7h222 \
    --filter SERVICE_CONTROL_POLICY
{
    "Policies": [
        {
            "Id": "p-FullAWSAccess",
```

```
            "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-
FullAWSAccess",
            "Name": "FullAWSAccess",
            "Description": "Allows access to every operation",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": true
        }
    ]
}
```

- AWSSDK: ListPoliciesForTarget

Mostrar todos los nodos raíz, unidades organizativas y cuentas que tienen una política asociada

Permisos mínimos

Para mostrar las entidades que tienen asociada una política, debe contar con el permiso siguiente:

- `organizations:ListTargetsForPolicy` con un elemento `Resource` en la misma instrucción de política que incluye el ARN de la política especificada (o "*")

AWS Management Console

Para enumerar todas las nodos raíz, unidades organizativas y cuentas que tienen asociada la política especificada

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaPolíticas, elija el tipo de política y, a continuación, elija el nombre de la política cuyos archivos adjuntos desea examinar.
3. Elija el iconoimplementaciónPara mostrar una tabla de cada raíz, unidad organizativa y cuenta a la que está asociada la política seleccionada.

AWS CLI & AWS SDKs

Para enumerar todas las nodos raíz, unidades organizativas y cuentas que tienen asociada la política especificada

Puede utilizar uno de los siguientes comandos para enumerar entidades que tengan una política:

- AWS CLI:list-targets-for-policy

  En el ejemplo siguiente se muestran todos los datos adjuntos a raíz, unidades organizativas y cuentas de la directiva especificada.

```
$ aws organizations list-targets-for-policy \
    --policy-id p-FullAWSAccess
{
    "Targets": [
        {
            "TargetId": "ou-a1b2-f6g7h111",
            "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h111",
            "Name": "testou2",
```

```
            "Type": "ORGANIZATIONAL_UNIT"
        },
        {
            "TargetId": "ou-a1b2-f6g7h222",
            "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
            "Name": "testou1",
            "Type": "ORGANIZATIONAL_UNIT"
        },
        {
            "TargetId": "123456789012",
            "Arn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
            "Name": "My Management Account (bisdavid)",
            "Type": "ACCOUNT"
        },
        {
            "TargetId": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "Type": "ROOT"
        }
    ]
}
```


- AWSSDK: ListTargetsForPolicy

Obtener información sobre una política

Permisos mínimos

Para mostrar los detalles de una política, debe contar con el permiso siguiente:

- `organizations:DescribePolicy` con un elemento `Resource` en la misma instrucción de política que incluye el ARN de la política especificada (o "*")

AWS Management Console

Para obtener información sobre una política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaPolíticas, elija el tipo de política de la política que desee examinar y, a continuación, elija el nombre de la política.

   La página de política muestra la información disponible sobre la política, incluido su ARN, descripción y destinos asociados.

   - LaContenidosmuestra el contenido actual de la política en formato JSON.
   - Laimplementaciónmuestra una lista de las nodos raíz, unidades organizativas y cuentas a los que está asociada la política.
   - LaTags (Etiquetas):muestra las etiquetas adjuntas a la directiva. Nota: la pestaña Etiquetas no está disponible paraAWSPolíticas administradas de.

   Para editar la directiva, elijaEdición de política de. Dado que cada tipo de directiva tiene requisitos de edición diferentes, consulte las instrucciones para crear y actualizar directivas del tipo de directiva especificado.

AWS CLI & AWS SDKs

Para obtener información sobre una política

Puede utilizar uno de los siguientes comandos para obtener detalles acerca de una política:

- AWS CLI:describe-policy

  En el siguiente ejemplo se muestran los detalles de la política especificada.

```
$ aws organizations describe-policy \
    --policy-id p-FullAWSAccess
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-FullAWSAccess",
            "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-
FullAWSAccess",
            "Name": "FullAWSAccess",
            "Description": "Allows access to every operation",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": true
        },
        "Content": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement\": [\n    {\n
    \"Effect\": \"Allow\",\n      \"Action\": \"*\",\n      \"Resource\": \"*\"\n
  }\n  ]\n}"
    }
}
```

- AWSSDK: DescribePolicy

Descripción de la herencia de políticas

Puede asociar políticas a entidades de organización (raíz de organización, unidad organizativa (OU) o cuenta) de su organización:

- Cuando se asocia una política a la raíz de la organización, todas las unidades organizativas y cuentas de la organización heredan esa política.
- Cuando asocia una política a una unidad organizativa específica, las cuentas que están directamente en esa unidad organizativa o cualquier unidad organizativa secundaria heredan la política.
- Cuando se asocia una política a una cuenta específica, solo afecta a esa cuenta.

Dado que puede asociar políticas a varios niveles de la organización, las cuentas pueden heredar varias políticas.

Cómo afectan las políticas exactamente a las unidades organizativas y a las cuentas que las heredan depende del tipo de política:

- Políticas de control de servicios (SCP) (p. 95)
- Tipos de políticas de administración (p. 97)
  - Políticas de exclusión de servicios de IA
  - Políticas de copia de seguridad
  - Políticas de etiquetas

Herencia para políticas de control de servicios

Important

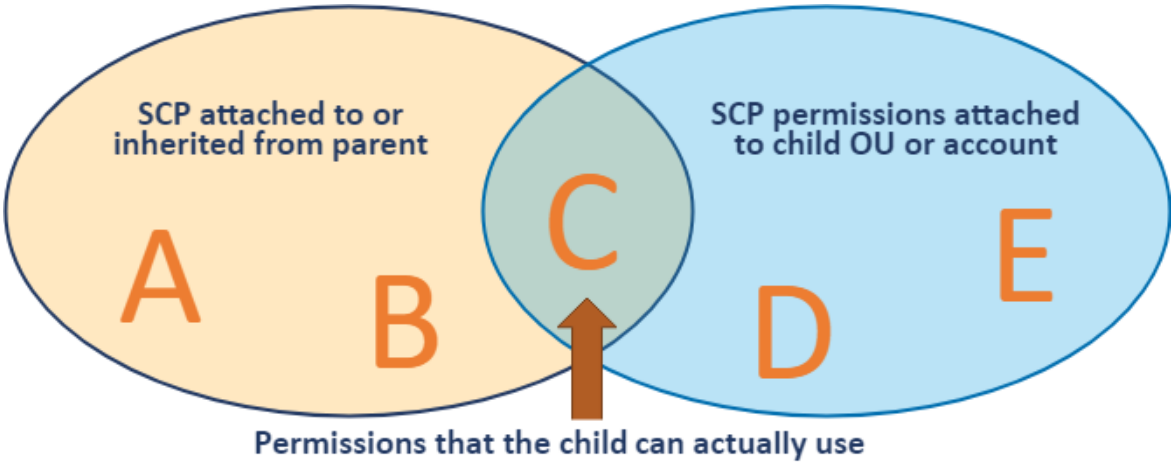
La información de esta sección hacenose aplican a los tipos de directivas de administración, incluidas las políticas de exclusión de servicios de IA, las políticas de copia de seguridad o las políticas de etiqueta. Consulte la siguiente sección Sintaxis y herencia de políticas para tipos de políticas de administración (p. 97).

Políticas de control de servicios (SCP)

La herencia de las políticas de control de servicios se comporta como un filtro a través del cual los permisos fluyen a todas las partes del árbol que se muestra a continuación. Imagine que la estructura de árbol invertido de la organización está compuesta por ramas que se conectan desde la raíz a todas las unidades organizativas y terminan en las cuentas. Todos los permisos de AWS fluyen en la raíz del árbol. Dichos permisos deben pasar después de las SCP asociados a la raíz, las unidades organizativas y la cuenta para llegar a la entidad principal (un rol o usuario de IAM) que realiza una solicitud. Cada SCP puede filtrar los permisos que pasan a los niveles inferiores. Si una instrucción `Deny` bloquea una acción, se deniega el acceso a esa acción a todas las unidades organizativas y cuentas afectadas por esa SCP. Una SCP en un nivel inferior no puede agregar un permiso después de que una SCP lo bloquee en un nivel superior. Las SCP solo pueden filtrar; nunca agregan permisos.

Las SCP no admiten operadores de herencia que alteren la forma en que se heredan los elementos de la política por las unidades organizativas secundarias y las cuentas.

En la siguiente ilustración se muestra cómo funcionan las SCP (p. 108).



En esta ilustración, suponga que el óvalo de la izquierda representa un SCP que está unido a la raíz de la organización. Permite permisos A, B y C. La raíz contiene una unidad organizativa (OU) a la que se asocia una segunda SCP representada por el óvalo de la derecha. Ese segundo SCP permite los permisos C, D y E. Debido a que el SCP conectado a la raíz no permite D ni E, ninguna unidad organizativa o cuenta puede utilizarlos. Aunque la SCP conectada a la unidad organizativa permite explícitamente D y E, están bloqueados porque están bloqueados por el SCP conectado a la raíz. Como la política SCP de la unidad organizativa no permite A ni B, esos permisos estarán bloqueados para la unidad organizativa y todas sus cuentas o unidades organizativas secundarias. Sin embargo, otras unidades organizativas que podrían existir bajo la raíz pueden seguir permitiendo A y B.

A medida que recorre la jerarquía de unidades organizativas a la cuenta, el proceso del párrafo anterior se repite en cada unidad organizativa y, finalmente, con la cuenta. En cada nivel, el resultado de la evaluación en el padre se convierte en la política a la izquierda del diagrama y se compara con los SCP asociados a la unidad organizativa secundaria.

Por ejemplo, si fuera a bajar el árbol a una unidad organizativa secundaria llamada X, imagine que el óvalo de la izquierda representa los permisos heredados y efectivos permitidos por todos los SCP por encima de la OU X en la jerarquía. El óvalo de la derecha representa el SCP conectado a una unidad organizativa o un Cuenta de AWS contenida en OU X. De nuevo, la intersección de esos permisos es lo que está disponible para ser utilizado la entidad de la derecha. Si esa entidad es un Cuenta de AWS , entonces la intersección es el conjunto de permisos que se pueden conceder a los usuarios y roles de esa cuenta. Si la entidad es una unidad organizativa, la intersección es el conjunto de permisos que pueden heredar los hijos de esa unidad organizativa. Repita el proceso para cada nivel en la jerarquía de unidades organizativas hasta que llegue a la cuenta misma. Esa política efectiva final es la lista de permisos permitidos por cada SCP por encima de esa cuenta y adjuntos a ella.

Esto significa que para permitir unaAWSen el nivel de cuenta de miembro, debe permitir esa API enEVERYentre la cuenta de miembro y la raíz de su organización. Debe adjuntar SCPs a todos los niveles desde la raíz de su organización a la cuenta de miembro que permite que elAWS(como EC2:RunInstances). Para ello, puede utilizar una de las estrategias siguientes:

- AEstrategia de listas de denegación (p. 122)hace uso de la`FullAWSAccess`SCP que se adjunta de forma predeterminada a cada unidad organizativa y cuenta. Este SCP anula la denegación implícita predeterminada y permite explícitamente que todos los permisos fluyan desde la raíz a cada cuenta, a menos que deniegue explícitamente un permiso con un SCP adicional que cree y adjunte a la unidad organizativa o cuenta apropiada. Esta estrategia funciona porque un`deny`en una política siempre anula cualquier tipo de`allow`. Ninguna cuenta por debajo del nivel de la unidad organizativa con la política de denegación puede usar la API denegada, y no hay forma de volver a agregar el permiso más bajo en la jerarquía. Para obtener más información, consulte Uso de políticas SCP como lista de denegación (p. 122).
- UnaEstrategia de listas de permitidos (p. 123)tiene que eliminar el`FullAWSAccess`SCP que se adjunta de forma predeterminada a cada unidad organizativa y cuenta. Esto significa que no se permiten API en ningún lugar a menos que usted las permita explícitamente. Para permitir que una API de servicio funcione en un Cuenta de AWS , debe crear sus propios SCPs y adjuntarlos a la cuenta y a cada unidad organizativa por encima de ella, hasta e incluyendo la raíz. Cada SCP en la jerarquía, comenzando en la raíz, debe permitir explícitamente las API que desea que se puedan utilizar en las unidades organizativas y las cuentas debajo de ella. Esta estrategia funciona porque un`allow`en un SCP anula un`deny`. Para obtener más información, consulte Uso de políticas SCP como lista de permitidos (p. 123).

Para revisar cómo se evalúan las políticas en términos de permisos y denegaciones implícitos frente a explícitos, y qué anula qué, consulteDeterminar si una solicitud se permite o se deniega dentro de una cuenta.

A los usuarios y roles de las cuentas se les deben seguir concediendo permisos conAWS Identity and Access ManagementPolíticas de permisos de (IAM) asociadas a ellas o a sus grupos. Los SCPs solo determinan qué permisos sonavailableque serán concedidas por esas políticas. El usuario no puede realizar ninguna de las acciones que las SCP correspondientes no permitan. Las acciones permitidas por las SCP pueden realizarse si se concede permiso a un usuario o rol mediante alguna de las políticas de permisos de IAM.

Cuando asocia políticas SCP a la raíz de la organización, a las unidades organizativas o directamente a las cuentas, todas las políticas que afectan a una cuenta determinada se evalúan de forma conjunta con las mismas reglas que rigen las políticas de permisos de IAM:

- Los usuarios y roles de las cuentas afectadas no pueden realizar ninguna acción que se indique en la instrucción `Deny` del SCP. Una instrucción `Deny` explícita invalida cualquier declaración `Allow` que concedan otras SCP.
- Una acción que tenga una instrucción `Allow` explícita en una SCP (como la política SCP predeterminada "*" o cualquier otra SCP que llame a una acción o servicio determinados) se puede delegar a los usuarios y roles de las cuentas afectadas.

- Una acción que no esté permitida de forma explícita por una SCP se denegará implícitamente y no se podrá delegar a los usuarios o funciones de las cuentas afectadas.

De forma predeterminada, una SCP denominada `FullAWSAccess` se asocia a cada raíz de la organización, unidad organizativa y cuenta. Esta SCP predeterminada permite todas las acciones y todos los servicios. Por lo tanto, en una nueva organización, hasta que empiece a crear o manipular las SCP, todos los permisos de IAM existentes seguirán operando de la misma manera que lo hicieron. En cuanto aplique una SCP nueva o modificada a la raíz de la organización o unidad organizativa que contenga una cuenta, los permisos que los usuarios tengan en esa cuenta empezarán a filtrarse por la SCP. Los permisos que antes funcionaban ahora podrían denegarse si la SCP no los permite en todos los niveles de la jerarquía hasta la cuenta especificada.

Si deshabilita el tipo de política SCP en la raíz de la organización, todas las SCP se desconectarán automáticamente de todas las entidades de la raíz de la organización. Si vuelve a habilitar las políticas SCP en la raíz de la organización, se pierden todas las asignaciones originales y todas las entidades se restablecen para asociarse únicamente a la política SCP `FullAWSAccess` predeterminada.

Para obtener más información acerca de la sintaxis de las SCP, consulte Sintaxis de las políticas SCP (p. 124).

Puede ver una lista de todas las políticas aplicadas a una cuenta y de dónde procede esa política. Para ello, elija una cuenta en el cuadro de diálogoAWS Organizationsconsola de . En la página de detalles de la cuenta, elija Policies (Políticas) y, a continuación, Service Control Policies (Políticas de control de servicios) en el panel de detalles de la derecha. Es posible que la misma política se aplique a la cuenta varias veces porque la política se puede asociar a cualquiera o a todos los contenedores principales de la cuenta. La política en vigor que se aplica a la cuenta es la intersección de permisos permitidos de todas las políticas aplicables.

Para obtener más información acerca de cómo utilizar las SCP, consulte Políticas de control de servicios (p. 108).

Sintaxis y herencia de políticas para tipos de políticas de administración

> **Important**
>
> La información de esta sección no se aplica a las SCP. Consulte la sección anterior Herencia para políticas de control de servicios (p. 95).

Los tipos de políticas de administración incluyen:

- Políticas de exclusión de servicios de inteligencia artificial (IA) (p. 144)
- Políticas de copia de seguridad (p. 160)
- Políticas de etiquetas (p. 195)

La herencia se comporta de manera diferente para los tipos de políticas de administración y para los tipos de políticas de control de servicios. La sintaxis de tipos de políticas de administración incluyeOperadores de herenciaLas unidades organizativas secundarias y las cuentas permiten especificar con precisión qué elementos de las políticas principales se aplican y qué elementos pueden anularse o modificarse cuando se heredan las unidades organizativas secundarias y las cuentas.

La política en vigor es el conjunto de reglas que se heredan desde la raíz de la organización y las unidades organizativas junto con las asociadas directamente a la cuenta. La política en vigor especifica el conjunto final de reglas que se aplican a la cuenta. Puede ver la política en vigor de una cuenta que incluya el efecto de todos los operadores heredados en las políticas aplicadas. Para obtener más información, consulte Visualización de políticas de etiquetas en vigor (p. 212).

En esta sección se explica cómo se procesan las políticas principales y secundarias en la política en vigor de una cuenta.

Terminology

En este tema se utilizan los siguientes términos al analizar la herencia de políticas.

Herencia de políticas

La interacción de políticas en distintos niveles de una organización, desplazándose desde la raíz de nivel superior de la organización, bajando por la jerarquía de unidades organizativas (OU) a cuentas individuales.

Puede asociar políticas a la raíz de la organización, las unidades organizativas, las cuentas individuales y a cualquier combinación de estas entidades de organización. La herencia de políticas hace referencia a las políticas que se asocian a la raíz de la organización o a una unidad organizativa. Todas las cuentas que son miembros de la raíz de la organización o unidad organizativa donde se asocia una política heredan esa política.

Por ejemplo, cuando se asocian las políticas a la raíz de la organización, todas las cuentas de la organización heredan esa política. Esto se debe a que todas las cuentas de una organización siempre están bajo la raíz de la organización. Cuando asocia una política a una unidad organizativa específica, las cuentas que están directamente en esa unidad organizativa o cualquier unidad organizativa secundaria heredan esa política. Dado que puede asociar políticas a varios niveles de la organización, las cuentas pueden heredar varios documentos de políticas para un solo tipo de política.

Políticas principales

Políticas asociadas más alto en el árbol organizativo que las políticas asociadas a entidades más abajo en el árbol.

Por ejemplo, si asocia la política A a la raíz de la organización, es solo una política. Si también asocia la política B a una unidad organizativa debajo de esa raíz, la política A es la política principal de la política B. La política B es la política secundaria de la política A. La política A y la política B se fusionan para crear la política de etiquetas en vigor para las cuentas de la unidad organizativa.

Políticas secundarias

Políticas asociadas a un nivel inferior en el árbol de la organización con respecto a la política principal.

Políticas en vigor

El documento de políticas único final que especifica las reglas que se aplican a una cuenta. La política en vigor es la agregación de cualquier política de etiquetas que herede la cuenta, además de cualquier política de etiquetas que se asocie directamente a la cuenta. Por ejemplo, las política de etiquetas le permiten ver la política de etiquetas en vigor que se aplica a cualquiera de sus cuentas. Para obtener más información, consulte Visualización de políticas de etiquetas en vigor (p. 212).

Operadores de herencia (p. 98)

Operadores que controlan cómo se fusionan las políticas heredadas en una sola política efectiva. Se considera que estos operadores son una característica avanzada. Los autores de políticas experimentados pueden utilizarlas para limitar los cambios que puede realizar una política secundaria y cómo se combinan las configuraciones de las políticas.

Operadores de herencia

Los operadores de herencia controlan cómo se fusionan las políticas heredadas y las políticas de la cuenta con la política de etiquetas en vigor de la cuenta. Estos operadores incluyen operadores de configuración de valores y operadores de control secundarios.

Cuando se utiliza el editor visual en la consola de AWS Organizations, solo se puede utilizar el operador de `@@assign`. Se considera que los otros operadores son una característica avanzada. Para utilizar el resto operadores, debe crear manualmente la política JSON. Los autores de políticas con experiencia pueden utilizar los operadores de herencia para controlar qué valores de etiqueta se aplican a la política en vigor y limitar los cambios que pueden realizar las políticas secundarias.

Operadores de configuración de valores

Puede utilizar los operadores de configuración de valores para controlar cómo interactúa la política con sus políticas principales:

- `@@assign`–Sobreescribecualquier configuración de directiva heredada con la configuración especificada. Si la configuración especificada no se hereda, este operador la agrega a la política en vigor. Este operador se puede aplicar a cualquier configuración de política de cualquier tipo.
  - Para la configuración de un solo valor, este operador reemplaza el valor heredado por el valor especificado.
  - Para configuraciones de valores múltiples (matrices JSON), este operador elimina los valores heredados y los reemplaza con los valores especificados por esta política.
- `@@append`–Añadelos ajustes especificados (sin quitar ninguno) a los heredados. Si la configuración especificada no se hereda, este operador la agrega a la política en vigor. Puede utilizar este operador solo con configuraciones de varios valores.
  - Este operador agrega los valores especificados a cualquier valor de la matriz heredada.
- `@@remove`–EliminaSi existe, la configuración heredada especificada de la política en vigor. Puede utilizar este operador solo con configuraciones de varios valores.
  - Este operador quita solo los valores especificados de la matriz de valores heredados de las políticas principales. Otros valores pueden continuar existiendo en la matriz y pueden ser heredados por las políticas secundarias.

Operadores de control secundarios

El uso de operadores de control secundarios es opcional. Puede utilizar el operador `@@operators_allowed_for_child_policies` para controlar qué operadores de configuración de valores pueden utilizar las políticas secundarias. Puede permitir todos los operadores, algunos operadores específicos o ningún operador. De forma predeterminada, todos los operadores (`@@all`) están permitidos.

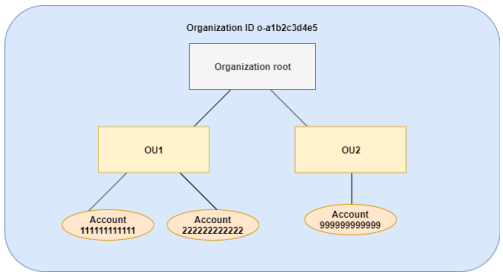
- `"@@operators_allowed_for_child_policies":["@@all"]`— Las unidades organizativas secundarias y las cuentas pueden utilizar cualquier operador en las políticas. De forma predeterminada, todos los operadores están permitidos en las políticas secundarias.
- `"@@operators_allowed_for_child_policies":["@@assign", "@@append", "@@remove"]`: las unidades organizativas secundarias y las cuentas solo pueden utilizar los operadores especificados en las directivas secundarias. Puede especificar uno o más operadores de configuración de valores en este operador de control secundario.
- `"@@operators_allowed_for_child_policies":["@@none"]`: las unidades organizativas secundarias y las cuentas no pueden utilizar operadores en las directivas. Puede usar este operador para bloquear eficazmente los valores definidos en una política principal de modo que las políticas secundarias no puedan agregar, anexar o quitar esos valores.

> **Note**
>
> Si un operador de control secundario heredado limita el uso de un operador, no puede revertir esa regla en una política secundaria. Si incluye operadores de control secundarios en una política principal, limitan los operadores de configuración de valores en todas las políticas secundarias.

Ejemplos de herencia de políticas

Estos ejemplos muestran cómo la herencia de políticas funciona al mostrar que las políticas de etiquetas principales y secundarias se fusionan en una política de etiquetas en vigor para una cuenta.

En los ejemplos se supone que tiene la estructura de organización que se muestra en el siguiente diagrama.



Ejemplos

- Ejemplo 1: Permitir que las políticas secundarias sobrescribanonlyValores de etiquetas (p. 100)
- Ejemplo 2: Agregar nuevos valores a las etiquetas heredadas (p. 101)
- Ejemplo 3: REMOVE valores de etiquetas heredadas (p. 103)
- Ejemplo 4: Restringir los cambios en las políticas (p. 104)
- Ejemplo 5: Conflictos con los operadores de control secundarios (p. 106)
- Ejemplo 6: Conflictos con valores de anexar en el mismo nivel de jerarquía (p. 107)

Ejemplo 1: Permitir que las políticas secundarias sobrescribanonlyValores de etiquetas

La siguiente política de etiquetas define la clave de etiquetas `CostCenter` y dos valores aceptables, `Development` y `Support`. Si asocia una política de etiquetas a la raíz de la organización, la política de etiquetas se encuentra en vigor para todas las cuentas en la organización.

Directiva A: directiva de etiqueta raíz de la organización

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

Suponga que desea que los usuarios en OU1 utilicen un valor de etiqueta diferente para una clave y desea aplicar la política de etiquetas para tipos de recursos específicos. Dado que la política A no especifica qué operadores de control secundarios están permitidos, todos los operadores están permitidos. Puede utilizar el operador `@@assign` y crear una política de etiquetas como la siguiente para asociar a OU1.

Directiva B — Política de etiqueta OU1

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Sandbox"
                ]
            },
            "enforced_for": {
                "@@assign": [
                    "redshift:*",
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

Al especificar el operador `@@assign` para la etiqueta, se hace lo siguiente cuando la política A y la B se fusionan para formar la política de etiquetas en vigor para una cuenta:

- La política B sobrescribe los dos valores de etiquetas que se especificaron en la política principal, la política A. El resultado es que `Sandbox` es el único valor compatible para la clave de etiquetas `CostCenter`.
- La adición de`enforced_for`Especifica que la propiedad`CostCenter`etiquetadebeDebe utilizar el valor de etiquetas especificado en todos los recursos de Amazon Redshift y las tablas de Amazon DynamoDB.

Como se muestra en el diagrama, OU1 incluye dos cuentas: 111111111111 y 222222222222.

Política de etiquetas en vigor resultante para las cuentas 111111111111 y 222222222222

> **Note**
>
> No puede utilizar directamente el contenido de una directiva efectiva mostrada como contenido de una nueva directiva. La sintaxis no incluye los operadores necesarios para controlar la fusión con otras directivas secundarias y primarias. La presentación de una política eficaz sólo tiene por objeto comprender los resultados de la fusión.

```
{
    "tags": {
        "costcenter": {
            "tag_key": "CostCenter",
            "tag_value": [
                "Sandbox"
            ],
            "enforced_for": [
                "redshift:*",
                "dynamodb:table"
            ]
        }
    }
}
```

Ejemplo 2: Agregar nuevos valores a las etiquetas heredadas

Puede haber casos en los que desee que todas las cuentas de su organización especifiquen una clave de etiquetas con una breve lista de valores aceptables. Para las cuentas de una unidad organizativa, es posible que desee permitir un valor adicional que solo puedan especificar esas cuentas al crear recursos.

En este ejemplo se especifica cómo hacerlo mediante el operador `@@append`. El operador `@@append` es una característica avanzada.

Al igual que el ejemplo 1, este ejemplo comienza con la política A para la política de etiquetas de la raíz de la organización.

Directiva A: directiva de etiqueta raíz de la organización

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

Para este ejemplo, asocie la política C a OU2. La diferencia en este ejemplo es que el uso del operador `@@append` en la política C agrega, en lugar de sobrescribir, la lista de valores aceptables y la regla `enforced_for`.

Directiva C — Política de etiqueta OU2 para anexar valores

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@append": [
                    "Marketing"
                ]
            },
            "enforced_for": {
                "@@append": [
                    "redshift:*",
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

La asociación de la política C a OU2 tiene los siguientes efectos cuando las políticas A y C se fusionan para formar la política de etiquetas en vigor para una cuenta:

- Dado que la política C incluye al operador `@@append`, permite agregar, no sobrescribir, la lista de valores de etiquetas aceptables especificados en la política A.
- Al igual que en la política B, la adición de`enforced_for`Especifica que la propiedad`CostCenter`Debe utilizarse como valor de etiquetas especificado en todos los recursos de Amazon Redshift y las tablas de Amazon DynamoDB. La sobrescritura (`@@assign`) y la adición (`@@append`) tienen el mismo efecto si la política principal no incluye un operador de control secundario que restringe lo que puede especificar una política secundaria.

Como se muestra en el diagrama, OU2 incluye una cuenta: 999999999999. Las políticas A y C se fusionan para crear la política de etiquetas en vigor para la cuenta 999999999999.

Política de etiquetas en vigor para la cuenta 999999999999

> **Note**
>
> No puede utilizar directamente el contenido de una directiva efectiva mostrada como contenido de una nueva directiva. La sintaxis no incluye los operadores necesarios para controlar la fusión con otras directivas secundarias y primarias. La presentación de una política eficaz sólo tiene por objeto comprender los resultados de la fusión.

```
{
    "tags": {
        "costcenter": {
            "tag_key": "CostCenter",
            "tag_value": [
                "Development",
                "Support",
                "Marketing"
            ],
            "enforced_for": [
                "redshift:*",
                "dynamodb:table"
            ]
        }
    }
}
```

Ejemplo 3: REMOVE valores de etiquetas heredadas

Puede haber casos en los que la política de etiquetas asociada a la organización defina más valores de etiquetas de los que desea utilizar una cuenta. En este ejemplo se explica cómo revisar una política de etiquetas mediante el operador `@@remove`. `@@remove` es una característica avanzada.

Al igual que otros ejemplos, este ejemplo comienza con la política A para la política de etiquetas de la raíz de la organización.

Directiva A: directiva de etiqueta raíz de la organización

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

Para este ejemplo, asocie la política D a la cuenta 999999999999.

Directiva D: directiva de etiqueta de la cuenta 9999999999 para eliminar valores

```
{
    "tags": {
```

```
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@remove": [
                    "Development",
                    "Marketing"
                ],
                "enforced_for": {
                    "@@remove": [
                        "redshift:*",
                        "dynamodb:table"
                    ]
                }
            }
        }
    }
}
```

La asociación de la política D a la cuenta 999999999999 tiene los siguientes efectos cuando las políticas A, C y D se fusionan para formar la política de etiquetas en vigor:

- Suponiendo que haya llevado a cabo todos los ejemplos anteriores, las políticas B, C y D son políticas secundarias de la política A. La política B solo se asocia a OU1, por lo que no tiene ningún efecto en la cuenta 9999999999999.
- Para la cuenta 9999999999999, el único valor aceptable para la clave de etiquetas `CostCenter` es `Support`.
- La conformidad no se aplica para la clave de etiquetas `CostCenter`.

Nueva política de etiquetas en vigor para la cuenta 999999999999

> **Note**
>
> No puede utilizar directamente el contenido de una directiva efectiva mostrada como contenido de una nueva directiva. La sintaxis no incluye los operadores necesarios para controlar la fusión con otras directivas secundarias y primarias. La presentación de una política eficaz sólo tiene por objeto comprender los resultados de la fusión.

```
{
    "tags": {
        "costcenter": {
            "tag_key": "CostCenter",
            "tag_value": [
                "Support"
            ]
        }
    }
}
```

Si posteriormente agrega más cuentas a OU2, sus políticas de etiquetas en vigor serían diferentes para la cuenta 999999999999. Esto se debe a que la política D más restrictiva solo se asocia a la cuenta y no a la unidad organizativa.

Ejemplo 4: Restringir los cambios en las políticas

Puede haber casos en los que desee restringir los cambios en las políticas secundarias. En este ejemplo se explica cómo hacerlo mediante los operadores de control secundarios.

Este ejemplo comienza con una nueva política de etiquetas de la raíz de la organización y se supone que las políticas de etiquetas aún no se asocian a las entidades de la organización.

Directiva E: directiva de etiqueta raíz de la organización para restringir los cambios en las directivas secundarias

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "Project"
            },
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append"],
                "@@assign": [
                    "Maintenance",
                    "Escalations"
                ]
            }
        }
    }
}
```

Cuando se asocia la política E a la raíz de la organización, la política impide que las políticas secundarias cambien la clave de la etiqueta `Project`. Sin embargo, las políticas secundarias pueden sobrescribir o anexar valores de etiquetas.

Supongamos que, a continuación, asocia la siguiente política F a una unidad organizativa.

Directiva F — Directiva de etiqueta de unidad organizativa

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@assign": "PROJECT"
            },
            "tag_value": {
                "@@append": [
                    "Escalations - research"
                ]
            }
        }
    }
}
```

La fusión de las políticas E y F tiene los siguientes efectos en las cuentas de la unidad organizativa:

- La política F es una política secundaria de la política E.
- La política F intenta cambiar el tratamiento del caso, pero no puede. Esto se debe a que la política E incluye el operador `"@@operators_allowed_for_child_policies": ["@@none"]` para la clave de etiqueta.
- Sin embargo, la política F puede añadir los valores de etiquetas para la clave. Esto se debe a que la política E incluye `"@@operators_allowed_for_child_policies": ["@@append"]` para el valor de etiqueta.

Política en vigor para las cuentas en la unidad organizativa

> **Note**
>
> No puede utilizar directamente el contenido de una directiva efectiva mostrada como contenido de una nueva directiva. La sintaxis no incluye los operadores necesarios para controlar la fusión

con otras directivas secundarias y primarias. La presentación de una política eficaz sólo tiene por objeto comprender los resultados de la fusión.

```
{
    "tags": {
        "project": {
            "tag_key": "project",
            "tag_value": [
                "Maintenance",
                "Escalations",
                "Escalations - research"
            ]
        }
    }
}
```

Ejemplo 5: Conflictos con los operadores de control secundarios

Los operadores de control secundarios pueden existir en políticas de etiquetas asociadas al mismo nivel en la jerarquía de la organización. Cuando eso sucede, se utiliza la intersección de los operadores permitidos cuando las políticas se fusionan para formar la política efectiva para las cuentas.

Supongamos que las políticas G y H se asocian a la raíz de la organización.

Directiva G: directiva 1 de etiqueta raíz de la organización

```
{
    "tags": {
        "project": {
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append"],
                "@@assign": [
                    "Maintenance"
                ]
            }
        }
    }
}
```

Directiva H: directiva 2 de etiqueta raíz de la organización

```
{
    "tags": {
        "project": {
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append", "@@remove"]
            }
        }
    }
}
```

En este ejemplo, una política en la raíz de la organización define que los valores de la clave de etiquetas solo se pueden anexar. La otra política asociada a la raíz de la organización permite que las políticas secundarias anexen y eliminen valores. La intersección de estos dos permisos se utiliza para las políticas secundarias. El resultado es que las políticas secundarias pueden anexar valores, pero no eliminar valores. Por lo tanto, la política secundaria puede anexar un valor a la lista de valores de etiquetas, pero no puede eliminar el valor `Maintenance`.

Ejemplo 6: Conflictos con valores de anexar en el mismo nivel de jerarquía

Puede asociar varias políticas de etiquetas a cada entidad de la organización. Al hacerlo, las políticas de etiqueta asociadas a la misma entidad de la organización podrían incluir información conflictiva. Las políticas se evalúan en función del orden en que se asociaron a la entidad de la organización. Para cambiar la política que se evalúa primero, puede asociar una política y, a continuación, volver a asociarla.

Supongamos que la política J se asocia primero a la raíz de la organización y, a continuación, la política K se asocia a la raíz de la organización.

Primera política de etiquetas asociada a la raíz de la organización

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@assign": "PROJECT"
            },
            "tag_value": {
                "@@append": ["Maintenance"]
            }
        }
    }
}
```

Política K: Segunda política de etiquetas asociada a la raíz de la organización

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@assign": "project"
            }
        }
    }
}
```

En este ejemplo, la clave de etiquetas `PROJECT` se utiliza en la política de etiquetas en vigor porque la política que la definió se asoció primero a la raíz de la organización.

Política JK: Política de etiquetas en vigor para la cuenta

La política en vigor para la cuenta es la siguiente.

> **Note**
>
> No puede utilizar directamente el contenido de una directiva efectiva mostrada como contenido de una nueva directiva. La sintaxis no incluye los operadores necesarios para controlar la fusión con otras directivas secundarias y primarias. La presentación de una política eficaz sólo tiene por objeto comprender los resultados de la fusión.

```
{
    "tags": {
        "project": {
            "tag_key": " PROJECT",
            "tag_value": [
                "Maintenance",
                "Escalations"
            ]
        }
```

```
    }
}
```

Políticas de control de servicios

Para obtener información y procedimientos comunes a todos los tipos de políticas, consulte los siguientes temas:

- Habilitar y desactivar tipos de políticas (p. 87)
- Obtenga detalles sobre las políticas (p. 90)
- Sintaxis y herencia de políticas (p. 95)

Políticas de control de servicios (SCP)

Las políticas de control de servicios (SCP) son un tipo de política de organización que puede utilizar para administrar permisos en su organización. Las políticas de control de servicios (SCP) ofrecen un control central sobre los máximos permisos disponibles para todas las cuentas de su organización. Las políticas de control de servicios le ayudan a garantizar que sus cuentas se mantengan dentro de las directrices de control de acceso de su organización. Las SCP solo están disponibles en las organizaciones que tienen todas las características habilitadas (p. 37). Las SCP no están disponibles si su organización ha habilitado únicamente las características de facturación unificada. Para obtener instrucciones sobre cómo habilitar SCP, consulte Habilitar y deshabilitar tipos de política (p. 87).

Las SCP por sí solas no son suficientes para conceder permisos a las cuentas de la organización. Un SCP no concede permisos. Un SCP define una barandilla o establece límites en las acciones que el administrador de la cuenta puede delegar a los usuarios de IAM y roles en las cuentas afectadas. El administrador aún debe adjuntarPolíticas basadas en identidad o políticas basadas en recursosa los usuarios o roles de IAM, o a los recursos de sus cuentas para conceder permisos realmente. LaPermisos efectivos (p. 109)son la intersección lógica entre lo que permite el SCP y lo que permite la IAM y las políticas basadas en recursos.

> **Important**
>
> Las SCP no afectan a los usuarios ni a los roles de la cuenta de administración. Afectan únicamente a las cuentas miembro de la organización.

Temas en esta página

Comprobación de los efectos de las políticas SCP

AWS recomienda encarecidamente no adjuntar SCP al nodo raíz de la organización sin haber comprobado exhaustivamente el impacto que tendrá la política en las cuentas. En lugar de ello, cree una unidad organizativa en la que pueda mover sus cuentas de una en una, o al menos en incrementos pequeños, a fin de garantizar que no bloquee inadvertidamente a los usuarios de servicios clave. Una forma de

determinar si una cuenta utiliza un servicio es examinar laLos datos del último acceso a los servicios en IAM. Otra forma es utilizar AWS CloudTrail para registrar el uso del servicio en el nivel de API.

Tamaño máximo de las políticas SCP

Todos los caracteres de la SCP se contabilizan para calcular su tamaño máximo (p. 330). Los ejemplos que aparecen en esta guía muestran los SCP formateados con espacios en blanco adicionales para mejorar su legibilidad. Sin embargo, para ahorrar espacio si el tamaño de la política se aproxima al tamaño máximo, puede eliminar todos los espacios en blanco, como espacios y saltos de línea, que estén fuera de las comillas.

> Tip
>
> Utilice el editor visual para crear la SCP. Este elimina automáticamente el espacio en blanco adicional.

Herencia de SCP en la jeraquía OU

Para obtener una explicación detallada de cómo funciona la herencia de SCP, consulteHerencia para políticas de control de servicios (p. 95)

Efectos en los permisos

Los SCP son similares aAWS Identity and Access Management(IAM) y utilizan casi la misma sintaxis. Sin embargo, una SCP nunca concede permisos. En su lugar, las SCP son políticas JSON que especifican los permisos máximos para las cuentas afectadas. Para obtener más información, consulteLógica de evaluación de políticasen laGuía del usuario de IAM.

- SCPafectan sólo a los usuarios y roles de IAMAdministración de cuentas que forman parte de la organización. Las SCP no afectan directamente a las políticas basadas en recursos. Tampoco afectan a los usuarios ni a los roles de cuentas que no pertenecen a la organización. Por ejemplo, tomemos el caso de un bucket de Amazon S3 que es propiedad de la cuenta A de una organización. La política de bucket (basada en recursos) concede acceso a los usuarios de la cuenta B de fuera de la organización. La cuenta A tiene asociada una SCP. Esta SCP no se aplica a los usuarios externos de la cuenta B. Solo se aplica a los usuarios que administra la cuenta A de la organización.
- Una SCP limita los permisos para los usuarios y roles de IAM de las cuentas miembro, incluido el usuario raíz de la cuenta miembro. Cada cuenta tiene únicamente los permisos concedidos por cada elemento principal situado por encima de ella. Si se bloquea un permiso en cualquier nivel por encima de la cuenta, ya sea implícitamente (sin incluirlo en una instrucción de política "`Allow`") o explícitamente (incluyéndolo en una instrucción de política "`Deny`"), el usuario o función de la cuenta afectada no puede usar ese permiso, aunque el administrador de la cuenta asocie la política de IAM `AdministratorAccess` con los permisos */* al usuario.
- Solo afectan a las SCPmemberCuentas de la organización. No tienen ningún efecto en los usuarios o roles de la cuenta de administración.
- A los usuarios y roles se les deben seguir concediendo permisos con las políticas de permisos de IAM adecuadas. Un usuario sin políticas de permisos de IAM no tendrá ningún tipo de acceso, aunque las políticas SCP correspondientes permitan todos los servicios y todas las acciones.
- Si un usuario o función tiene una política de permisos de IAM que le concede acceso a una acción que también está permitida por las SCP correspondientes, el usuario o función puede realizar dicha acción.
- Si un usuario o función tiene una política de permisos de IAM que le concede acceso a una acción que no está permitida o ha sido explícitamente denegada por las SCP correspondientes, el usuario o función no puede realizar dicha acción.
- Las SCP afectan a todos los usuarios y roles en las cuentas adjuntas, incluyendo el usuario raíz. Las únicas excepciones son las descritas en Tareas y entidades no restringidas por SCP (p. 110).

- Las SCP no afectan a cualquier rol vinculado al servicio. Las funciones vinculadas a servicios permiten que otros servicios de AWS se integren con AWS Organizations y no se pueden restringir con SCP.
- Cuando se deshabilita el tipo de política SCP en un nodo raíz, todas las políticas SCP se desasocian automáticamente de todas las entidades de AWS Organizations de ese nodo raíz. Las entidades de AWS Organizations incluyen unidades organizativas, organizaciones y cuentas. Si vuelve a habilitar las políticas SCP en un nodo raíz, ese nodo se revierte a solo la política `FullAWSAccess` predeterminada asociada automáticamente a todas las entidades del nodo raíz. Se perderán todas las asociaciones de políticas SCP a las entidades de AWS Organizations realizadas antes de que se deshabilitaran las SCP y no podrán recuperarse automáticamente aunque las vuelva a asociar manualmente.
- Si existen tanto un límite de permisos (función de IAM avanzada) como una SCP, entonces el límite, la SCP y la política basada en identidad deben permitir la acción.

Uso de datos de acceso para mejorar las políticas SCP

Cuando haya iniciado sesión con credenciales de cuenta de administración, puede verLos datos del último acceso al serviciopara unAWS Organizationsentidad o política en elAWS OrganizationsEn la consola de IAM. También puede utilizar laAWS Command Line Interface(AWS CLI) oAWSEn IAM para recuperar datos de los últimos servicios a los que se ha accedido. Estos datos incluyen información sobre los servicios permitidos que los usuarios de IAM y las funciones de en unaAWS Organizationsúltima vez intentó acceder y cuándo. Puede utilizar esta información para identificar permisos no utilizado, de modo que pueda perfeccionar sus políticas de control de servicios para que cumplan mejor el principio de privilegios mínimos.

Por ejemplo, es posible que tenga una SCP de lista de denegación (p. 122) que prohíba el acceso a tres servicios de AWS. Todos los servicios que no figuren en la instrucción `Deny` de la SCP se permiten. Los datos del último acceso al servicio de en IAM le indican quéAWSLos servicios de están permitidos por la SCP pero nunca se utilizan. Con esa información, puede actualizar la SCP para denegar el acceso a los servicios que no necesite.

Para obtener más información, consulte los siguientes temas de la guía del usuario de IAM:

- Visualización de los datos del último acceso al servicio de Organizations
- Uso de datos para ajustar los permisos de una unidad organizativa

Tareas y entidades no restringidas por SCP

Ustedno puedeutilizar SCPs para restringir las siguientes tareas:

- Cualquier acción realizada por la cuenta de administración
- Cualquier acción realizada mediante permisos que adjuntos a una función vinculada al servicio
- Registrarse en el plan Enterprise Support como usuario raíz
- Cambiar el nivel de soporte de AWS como usuario raíz
- Administrar las claves de Amazon CloudFront como usuario raíz
- Proporcionar funcionalidad de signatario de confianza para contenido privado de CloudFront
- Configurar DNS inverso para un servidor de correo electrónico de Amazon LightSail como usuario raíz
- Tareas en algunosAWSServicios relacionados con:
  - Alexa Top Sites
  - Alexa Web Information Service
  - Amazon Mechanical Turk
  - API de marketing de productos de Amazon

Excepciones para cuentas de miembro creadas antes del 15 de septiembre de 2017

ParaAlgunoCreadas de cuentasAntes15 de septiembre de 2017no puedeutilizar SCPs para evitar que el usuario raíz de esas cuentas miembro realice las siguientes tareas:

> **Important**
>
> ParaTodoCreadas de cuentasDespués15 de septiembre de 2017, las siguientes excepciones no se aplican yCANutilizar SCPs para evitar que el usuario raíz de esas cuentas miembro realice las siguientes tareas. Sin embargo, a menos que esté seguro de queTodode las cuentas de su organización se crearon después del 15 de septiembre de 2017, le recomendamos que no confíe en las SCP para intentar restringir estas operaciones:

- Activar o desactivar la autenticación multifactor en el usuario raíz
- Crear, actualizar o eliminar las claves x.509 del usuario raíz
- Cambiar la contraseña del usuario raíz
- Crear, actualizar o eliminar claves de acceso raíz

Crear, actualizar y eliminar políticas de control de servicios

Cuando inicia sesión en la cuenta de administración de la organización, puede crear y actualizarPolíticas de control de servicios (SCP) (p. 108). Las SCP se crean mediante instrucciones que deniegan o permiten el acceso a los servicios y las acciones especificados.

La configuración predeterminada para trabajar con SCPs es usar una estrategia de «lista de bloques» donde todas las acciones están implícitamente permitidas excepto aquellas acciones que desea bloquear mediante la creación de sentencias que niegan el acceso. Con las instrucciones de denegación, puede especificar recursos y condiciones para la instrucción y utilizar laNotActionELEMENT. En las instrucciones de permiso, solo puede especificar servicios y acciones. Para obtener más información acerca de las instrucciones que deniegan el acceso y permiten el acceso, consulte Estrategias para usar políticas SCP (p. 121).

> **Tip**
>
> Puede usarLos datos del último acceso al servicioinIAMcomo punto de datos para actualizar las SCP para restringir el acceso a solo lasAWSlos servicios que necesita. Para obtener más información, consulteVisualización de los datos del último acceso al servicio de Organizationsen laGuía del usuario de IAM.

En este tema:

- Después de tiActivar políticas de control de servicios (p. 87)para su organización, puedeCrear una política. (p. 111).
- Cuando cambien sus requisitos de SCP, puedePara actualizar una política existente (p. 115).
- Cuando ya no necesite una política y después de desasociarla de todas las unidades organizativas (OU) y cuentas, puedeeliminarlo (p. 118).

Creación de una SCP

> **Permisos mínimos**
>
> Para crear las SCP, necesita permiso para ejecutar la siguiente acción:
>
> - `organizations:CreatePolicy`

AWS Management Console

Para crear una política de control de servicios

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la página Service control policies (Políticas de control de servicios), seleccione Create policy (Crear política).
3. En la páginaCreación de una nueva política de control de serviciospage, introduzca unNombre de la políticaUna opción opcionalDescripción de la política.
4. (Opcional) Para agregar una o varias etiquetas, elijaAgregue etiquetay, a continuación, introduzca una clave y un valor opcional. Dejar el valor en blanco lo establece en una cadena vacía; no es`null`. Puede asociar hasta 50 etiquetas a una política. Para obtener más información, consulte Etiquetado de recursos de AWS Organizations (p. 229).

   > **Note**
   >
   > En la mayoría de los pasos que siguen, discutimos el uso de los controles en el lado derecho del editor JSON para construir la política, elemento por elemento. Alternativamente, puede, en cualquier momento, simplemente ingresar texto en el editor JSON en el lado izquierdo de la ventana. Puede escribir directamente, o usar copiar y pegar.

5. Para crear la política, los siguientes pasos varían en función de si desea agregar una instrucción queniega (p. 122)orPermite (p. 123)Obtener acceso a. Para obtener más información, consulteEstrategias para usar políticas SCP (p. 121). Si usa`Deny`, tiene un control adicional porque puede restringir el acceso a recursos específicos, definir condiciones para cuándo las SCP están vigentes y utilizar la instrucciónNotActionELEMENT. Para obtener más detalles acerca de la sintaxis, consulteSintaxis de las políticas SCP (p. 124).

   Para añadir una instrucción que deniega el acceso:

   a. A la derechaEditar declaracióndel editor, en1. Agregue acciones, elija unAWSServicio

      A medida que elige opciones a la derecha, el editor de JSON se actualiza para mostrar la correspondiente política de JSON a la izquierda.

   b. Después de seleccionar un servicio, se abre una lista que contiene las acciones disponibles para ese servicio. Puede elegirTodas las accioneso elija una o varias acciones individuales que desea denegar.

      El JSON de la izquierda se actualiza para incluir las acciones seleccionadas.

      > **Note**
      >
      > Si selecciona una acción individual y luego también vuelve atrás y también seleccionaTodas las acciones, la entrada esperada para`servicename/*`se agrega al JSON, pero las acciones individuales que seleccionó anteriormente se dejan en el JSON y no se eliminan.

   c. Si desea añadir acciones desde servicios adicionales, puede elegirTodos los serviciosAl principio de laInstrucciónу, a continuación, repita los dos pasos anteriores según sea necesario.

   d. Especifique los recursos que hay que incluir en la instrucción.

      - Junto a2. Adición de un recurso, elijaAdd.
      - En el navegadorAdd resource (Añadir recurso)En la lista, elija el servicio de cuyos recursos desea controlar. Puede seleccionar entre solo los servicios que ha seleccionado en el paso anterior.

- UNDERTipo de recurso, elija el tipo de recurso que desea controlar.
- Por último, complete el nombre de recurso de Amazon (ARN) enARN de recursoPara identificar el recurso específico al que desea controlar el acceso. Debe reemplazar todos los marcadores de posición que estén rodeados de llaves`{}`. Puede especificar comodines (`*`) donde la sintaxis ARN de ese tipo de recurso lo permite. Consulte la documentación de un tipo de recurso específico para obtener información sobre dónde puede usar comodines.
- Guarde su adición a la política eligiendoAdd resource (Añadir recurso). La`Resource`en el JSON refleja sus adiciones o cambios. LaRecursoEl elemento es obligatorio.

  Tip

  Si desea especificar todos los recursos para el servicio seleccionado, elija laTodos los recursosen la lista, o edite el`Resource`directamente en el JSON para leer`"Resource":"*"`.

e. (Opcional) Para especificar las condiciones que limitan cuando una instrucción de política está en vigor, junto a3. Agregue condición, elijaAdd.

- Clave de condición— En la lista puede elegir cualquier clave de condición que esté disponible para todos losAWSServicios (por ejemplo,`aws:SourceIp`) o una clave específica de servicio para sólo uno de los servicios que ha seleccionado para esta instrucción.
- Qualifier— (Opcional) Si proporciona varios valores para la condición (dependiendo de la clave de condición especificada), puede especificar unCalificadorpara probar solicitudes con los valores.
  - Valor predeterminado: prueba un único valor de la solicitud con el valor de la clave de condición de la política. La condición devuelve true si el valor de la solicitud coincide con el valor de la política. Si la política especifica más de un valor, entonces se tratan como una prueba «o», y la condición devuelve true si los valores de solicitud coinciden con cualquiera de los valores de la política.
  - Para cualquier valor en una solicitud— Cuando la solicitud puede tener varios valores, esta opción prueba siAl menos unoDe los valores de solicitud coincide con al menos uno de los valores de clave de condición de la política. La condición devuelve true si alguno de los valores de clave de la solicitud coincide con alguno de los valores de condición de la política. Si no hay una clave coincidente o si hay un conjunto de datos es nulo, la condición devuelve "false".
  - Para todos los valores de una solicitud— Cuando la solicitud puede tener varios valores, esta opción prueba siCadacoincide con un valor de clave de condición en la política. La condición devuelve true si cada valor de clave de la solicitud coincide con al menos un valor de la política. También devuelve true si no hay claves en la solicitud o si los valores de clave se resuelven en un conjunto de datos nulo, como una cadena vacía.
- "."— Eloperadorespecifica el tipo de comparación que se va a realizar. Las opciones que se presentan dependen del tipo de datos de la clave de condición. Por ejemplo, el`aws:CurrentTime`le permite elegir entre cualquiera de los operadores de comparación de fechas, o`Null`, que puede usar para probar si el valor está presente en la solicitud.

  Para cualquier operador de condición excepto el`Null`Puede elegir la opciónIfExistsOpción.
- Valor— (Opcional) Especifique uno o varios valores para los que desea probar la solicitud.

Elija Add condition.

Para obtener más información acerca de las claves de condición, consulteElemento de política JSON de IAM: Condiciónen laGuía del usuario de IAM.

f. (Opcional) Para utilizar el`NotAction`elemento para denegar el acceso a todas las accionesExceptolos especificados, reemplace`Action`en el panel izquierdo con`NotAction`, justo después de la`"Effect": "Deny",`ELEMENT. Para obtener más información, consulteElemento de política JSON de IAM: NotActionen laGuía del usuario de IAM.

6. Para añadir una instrucción que permita el acceso:

   a. En el editor JSON de la izquierda, cambie la línea`"Effect": "Deny"`De a`"Effect": "Allow"`.

      A medida que elige opciones a la derecha, el editor de JSON se actualiza para mostrar la correspondiente política de JSON a la izquierda.

   b. Después de seleccionar un servicio, se abre una lista que contiene las acciones disponibles para ese servicio. Puede elegirTodas las accioneso bien elija una o varias acciones individuales que desea permitir.

      El JSON de la izquierda se actualiza para incluir las acciones seleccionadas.

      Note

      Si selecciona una acción individual y luego también vuelve atrás y también seleccionaTodas las acciones, la entrada esperada para*`servicename`*`/*`se agrega al JSON, pero las acciones individuales que seleccionó anteriormente se dejan en el JSON y no se eliminan.

   c. Si desea añadir acciones desde servicios adicionales, puede elegirTodos los serviciosAl principio de laInstruccióny, a continuación, repita los dos pasos anteriores según sea necesario.

7. (Opcional) Para agregar otra instrucción a la política, elijaAñadir declaracióny use el editor visual para crear la siguiente declaración.
8. Cuando haya terminado de añadir instrucciones, elija Create policy (Crear política) para guardar la SCP.

Su nueva SCP aparecerá en la lista de políticas de la organización. Ahora puede asociar la SCP a la raíz, a unidades organizativas o a cuentas (p. 119).

AWS CLI & AWS SDKs

Para crear una política de control de servicios

Puede utilizar uno de los siguientes comandos para crear una SCP:

- AWS CLI: create-policy

  En el siguiente ejemplo, se presupone que dispone de un archivo denominado`Deny-IAM.json`con el texto de la directiva JSON en él. Utiliza ese archivo para crear una nueva política de control de servicios.

```
$ aws organizations create-policy \
    --content file://Deny-IAM.json \
    --description "Deny all IAM actions" \
    --name DenyIAMSCP \
    --type SERVICE_CONTROL_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "DenyIAMSCP",
            "Description": "Deny all IAM actions",
```

```
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

- AWSSDK de: CreatePolicy

Note

Las SCP no se aplican en la cuenta de administración y en algunas otras situaciones. Para obtener más información, consulte Tareas y entidades no restringidas por SCP (p. 110).

Actualización de una SCP

Cuando inicia sesión en la cuenta de administración de su organización, puede cambiar el nombre o cambiar el contenido de una política. El cambio de contenido de una SCP afecta inmediatamente a los usuarios, grupos y roles de todas las cuentas asociadas.

Permisos mínimos

Para actualizar una SCP, necesita permiso para ejecutar las siguientes acciones:

- `organizations:UpdatePolicy` con un elemento `Resource` en la misma instrucción de política que incluye el ARN de la política especificada (o "*")
- `organizations:DescribePolicy` con un elemento `Resource` en la misma instrucción de política que incluye el ARN de la política especificada (o "*")

AWS Management Console

Para actualizar una política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaPolíticas de control de serviciosHaga clic en el nombre de la política que desea actualizar.
3. En la página de detalles de la política, elijaEditar política.
4. Realice una de las siguientes modificaciones, o todas:
   - Puede cambiar el nombre de la política introduciendo un nuevo nombre enNombre de la política.
   - Puede cambiar la descripción introduciendo nuevo texto enDescripción de la política.
   - Puede editar el texto de la directiva editando la directiva en formato JSON en el panel izquierdo. Alternativamente, puede elegir una instrucción en el editor de la izquierda y, a continuación, modificar sus elementos utilizando los controles de la izquierda. Para obtener más detalles acerca de cada control, consulte laCreación de un procedimiento SCP (p. 111)Anteriormente en este tema.
5. Cuando haya finalizado, Save changes (Guardar cambios).

AWS CLI & AWS SDKs

Para actualizar una política

Puede utilizar uno de los comandos siguientes para actualizar una política:

- AWS CLI:policy de actualización

  En el siguiente ejemplo se cambia el nombre de una política.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "MyRenamedPolicy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "Blocks all IAM actions",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

  En el siguiente ejemplo se agrega o cambia la descripción de una política de control de servicios.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new policy description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

  En el ejemplo siguiente se cambia el documento de directiva del SCP especificando un archivo que contiene el nuevo texto de directiva JSON.

```
$ aws organizations update-policy \
    --policy-id p-zlfw1r64
    --content file://MyNewPolicyText.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
```

```
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"AModifiedPolicy\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*
\"]}]}"
    }
}
```

- AWSSDK de: UpdatePolicy

Para obtener más información

Para obtener más información acerca de la creación de SCP, consulte los siguientes temas:

- Ejemplo de políticas de control de servicios (p. 131)
- Sintaxis de las políticas SCP (p. 124)

Edición de etiquetas enlazadas a un SCP

Cuando inicie sesión en la cuenta de administración de su organización, puede agregar o quitar las etiquetas adjuntas a un SCP. Para obtener más información acerca del etiquetado, consulte Etiquetado de recursos de AWS Organizations (p. 229).

Permisos mínimos

Para editar las etiquetas adjuntas a un SCP en suAWS, debe contar con los permisos siguientes:

- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:DescribePolicy`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

Para editar las etiquetas asociadas a un SCP

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaPolíticas de control de serviciosElija el nombre de la política con las etiquetas que desea editar.
3. En la página de detalles de política, elija la opciónTags (Etiquetas):Elija la pestaña y, a continuación, elijaAdministrar etiquetas.
4. Realice una de las siguientes modificaciones, o todas:
   - Para cambiar el valor de una etiqueta, escriba un nuevo valor sobre el anterior. No se puede modificar directamente la clave de etiqueta. Para cambiar una clave, debe eliminar la etiqueta con la clave anterior y, a continuación, agregar una etiqueta con la nueva clave.
   - Elimine una etiqueta existente seleccionandoRemove.
   - Agregue una nueva clave de etiqueta y un par de valor. SeleccionarAgregue etiquetay, a continuación, introduzca el nuevo nombre de clave y el valor opcional en los cuadros proporcionados. Si deja elValorEn el cuadro vacío, el valor es una cadena vacía; no es`null`.
5. Cuando haya finalizado, Save changes (Guardar cambios).

AWS CLI & AWS SDKs

Para editar las etiquetas asociadas a un SCP

Puede utilizar uno de los comandos siguientes para editar las etiquetas asociadas a una SCP:

- AWS CLI:tag-resourceyuntag-resource
- AWSSDK de: TagResourceyUntagResource

Eliminación de una SCP

Cuando inicia sesión en la cuenta de administración de su organización, puede eliminar una política que ya no necesite de su organización.

Notes

- Para poder eliminar una política, primero debe desasociarla de todas las entidades asociadas.
- No puede eliminar ningunaAWSSCP administrado, como el SCP llamado`FullAWSAccess`.

Permisos mínimos

Para eliminar una SCP, necesita permiso para ejecutar la siguiente acción:

- `organizations:DeletePolicy`

AWS Management Console

Para eliminar un SCP

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaPolíticas de control de servicios, elija el nombre del SCP que desea eliminar.
3. Debe desasociar primero la política que desea eliminar de todas las raíces, las unidades organizativas y las cuentas. Elija el iconoimplementación, elija el botón de opción situado junto a cada raíz, unidad organizativa o cuenta que se muestra en laimplementaciónElija la lista y, a continuación, elijaSeparar. En el cuadro de diálogo de confirmación, elijaSeparar. Repita la operación hasta que elimine todos los destinos.
4. SeleccionarEliminarAl principio de la página.
5. En el cuadro de diálogo de confirmación, escriba el nombre de la política y, a continuación, elijaEliminar.

AWS CLI & AWS SDKs

Para eliminar un SCP

Puede utilizar uno de los comandos siguientes para eliminar una política:

- AWS CLI: delete-policy

  En el siguiente ejemplo se elimina el SCP especificado.

```
$ aws organizations delete-policy \
    --policy-id p-i9j8k7l6m5
```

  Este comando no genera ninguna salida cuando se realiza correctamente.

- AWSSDK de: DeletePolicy

Asociar y separar políticas de control de servicios

Cuando inicia sesión en la cuenta de administración de su organización, puede asociar una política de control de servicios (SCP) que haya creado anteriormente. Puede asociar una SCP a la raíz de la organización, a una unidad organizativa (OU) o directamente a una cuenta. Para asociar una SCP, siga los pasos que se describen a continuación.

Permisos mínimos

Para asociar una SCP a un nodo raíz, una unidad organizativa o una cuenta, necesita permiso para ejecutar la siguiente acción:

- `organizations:AttachPolicy`con un`Resource`en la misma declaración de política que incluye «*» o el nombre de recurso de Amazon (ARN) de la política especificada y el ARN de la raíz, unidad organizativa o cuenta a la que desea adjuntar la política

AWS Management Console

Puede asociar una SCP navegando por la política o al nodo raíz, unidad organizativa o cuenta a la que desea asociar la política.

Para asociar una SCP navegando hasta la raíz, la unidad organizativa o la cuenta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la página Cuentas de AWS A continuación, seleccione la casilla de verificación situada junto a la raíz, unidad organizativa o cuenta a la que desea asociar una SCP. Es posible que tenga que expandir las unidades organizativas (elija la opción▶) para encontrar la unidad organizativa o la cuenta que desea.
3. En el navegadorPolíticas, en la entrada dePolíticas de control de servicios, elijaAttach.
4. Busque la política que desea y elijaAsociar política.

   La lista de SCP asociadas en laPolíticasse actualiza para incluir la nueva adición. Este cambio de política tiene efecto inmediatamente, afectando a los permisos de los usuarios y roles de IAM de la cuenta asociada o de todas las cuentas situadas bajo el nodo raíz o la unidad organizativa.

Para adjuntar un SCP navegando a la directiva

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaPolíticas de control de servicios, elija el nombre de la política que desea asociar.
3. En la páginaimplementación, elija.Attach.
4. Elija el botón de opción situado junto a la raíz, unidad organizativa o cuenta a la que desea asociar la política. Es posible que tenga que expandir las unidades organizativas (elija la opción▶) para encontrar la unidad organizativa o la cuenta que desea.
5. Elija Attach policy (Asociar política).

   La lista de SCP asociadas en laimplementaciónse actualiza para incluir la nueva adición. Este cambio de política tiene efecto inmediatamente, afectando a los permisos de los usuarios y roles de IAM de la cuenta asociada o de todas las cuentas situadas bajo el nodo raíz o la unidad organizativa.

AWS CLI & AWS SDKs

Para asociar una SCP navegando hasta la raíz, la unidad organizativa o la cuenta

Puede utilizar uno de los comandos siguientes para asociar una SCP:

- AWS CLI:attach-policy

  En el ejemplo siguiente se adjunta un SCP a una unidad organizativa.

```
$ aws organizations attach-policy \
    --policy-id p-i9j8k7l6m5 \
    --target-id ou-a1b2-f6g7h222
```

  Este comando no genera ninguna salida cuando se realiza correctamente.
- AWSSDK de: AttachPolicy

Este cambio de política tiene efecto inmediatamente, afectando a los permisos de los usuarios y roles de IAM de la cuenta asociada o de todas las cuentas situadas bajo el nodo raíz o la unidad organizativa.

Desasociación de una política SCP de la raíz de la organización, las unidades organizativas o las cuentas

Cuando inicia sesión en la cuenta de administración de su organización, puede desasociar una SCP de la raíz de la organización, unidad organizativa o cuenta a la que está asociada. Después de desasociar una SCP de una entidad, dicha SCP ya no se aplica a ninguna cuenta que estuviera afectada por la entidad ahora desasociada. Para desasociar una SCP, siga los pasos que se describen a continuación.

Note

No puede separar la última política SCP de una raíz, una unidad organizativa o una cuenta. Debe haber al menos una SCP asociada a cada raíz, unidad organizativa y cuenta en todo momento.

Permisos mínimos

Para desasociar una SCP de la raíz, unidad organizativa o cuenta, necesita permiso para ejecutar la siguiente acción:

- `organizations:DetachPolicy`

AWS Management Console

Puede desasociar una SCP desplazándose a la política o al nodo raíz, unidad organizativa o cuenta desde la que desea adjuntar la política.

Para desasociar una SCP navegando a la raíz, la unidad organizativa o la cuenta a la que está asociada

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la página Cuentas de AWS Vaya a la raíz, la unidad organizativa o la cuenta de la que desea desasociar una política. Es posible que tenga que expandir las unidades organizativas (elija la opción▶) para encontrar la unidad organizativa o la cuenta que desea. Elija el nombre de la raíz, la unidad organizativa o la cuenta.

3. En la páginaPolíticas, elija el botón de opción situado junto al SCP que desea desasociar y, a continuación, elijaSeparar.
4. En el cuadro de diálogo de confirmación, elijaPolítica de desvinculación.

   La lista de SCP asociadas se actualiza. El cambio de políticas que se origina al desasociar el SCP entra en vigor inmediatamente. Por ejemplo, cuando se desasocia una SCP, este cambio afecta inmediatamente a los permisos de los usuarios y roles de IAM de de la cuenta o cuentas anteriormente asociadas situados bajo el nodo raíz de la organización o unidad organizativa anteriormente asociados.

Para desasociar un SCP navegando a la directiva

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaPolíticas de control de servicios, elija el nombre de la política que desea desasociar de una raíz, una unidad organizativa o una cuenta.
3. En la páginaimplementaciónSeleccione el botón de opción situado junto a la raíz, unidad organizativa o cuenta de la que desea desasociar la política. Es posible que tenga que expandir las unidades organizativas (elija la opción ▶) para encontrar la unidad organizativa o la cuenta que desea.
4. Elija Detach (Desasociar).
5. En el cuadro de diálogo de confirmación, elijaSeparar.

   La lista de SCP asociadas se actualiza. El cambio de políticas que se origina al desasociar el SCP entra en vigor inmediatamente. Por ejemplo, cuando se desasocia una SCP, este cambio afecta inmediatamente a los permisos de los usuarios y roles de IAM de de la cuenta o cuentas anteriormente asociadas situados bajo el nodo raíz de la organización o unidad organizativa anteriormente asociados.

AWS CLI & AWS SDKs

Para desasociar un SCP de una raíz, unidad organizativa o cuenta

Puede utilizar uno de los comandos siguientes para desasociar una SCP:

- AWS CLI:detach-policy

  En el ejemplo siguiente se desconecta el SCP especificado de la unidad organizativa especificada.

```
$ aws organizations detach-policy \
    --policy-id p-i9j8k7l6m5 \
    --target-id ou-a1b2-f6g7h222
```

- AWSSDK de: DetachPolicy

Esta modificación de política tiene efecto inmediatamente, afectando a los permisos de los usuarios y roles de IAM de la cuenta asociada o de todas las cuentas situadas bajo el nodo raíz o la unidad organizativa.

Estrategias para usar políticas SCP

Puede configurar las políticas de control de servicios (SCP) de su organización para que funcionen de alguna de las maneras siguientes:

- ALista de denegación (p. 122): las acciones están permitidas de forma predeterminada y usted especifica los servicios y las acciones que están prohibidos.
- UnaLista de permitidos (p. 123): las acciones están prohibidas de forma predeterminada y usted especifica los servicios y las acciones que se permiten.

> Tip
>
> Puede usarLos datos del último acceso al servicioinIAMPara actualizar las SCP para restringir el acceso a solo lasAWSlos servicios que necesita. Para obtener más información, consulteVisualización de los datos del último acceso al servicio de Organizationsen laGuía del usuario de IAM.

Uso de políticas SCP como lista de denegación

La configuración predeterminada de AWS Organizations permite usar las SCP como listas de denegación. Los administradores de cuentas pueden usar una estrategia de listas de denegación para delegar todos los servicios y acciones hasta que haya creado y adjuntado una SCP que deniegue el acceso a un servicio concreto o a un conjunto de acciones. El uso de instrucciones de denegación requiere menos mantenimiento, porque no es preciso actualizarlas cada vez que AWS añade nuevos servicios. Las instrucciones de denegación suelen ocupar menos espacio, de modo que es más fácil respetar el tamaño máximo para los SCP (p. 330). En una instrucción cuyo elemento `Effect` tiene el valor `Deny`, también puede restringir el acceso a recursos concretos o definir las condiciones que determinan cuándo se aplicarán las SCP.

Para que esto sea posible, AWS Organizations asocia una SCP administrada por AWS denominada FullAWSAccess a cada nodo raíz y unidad organizativa en el momento de su creación. Esta política permite todos los servicios y acciones. Siempre está disponible para que la asocie o desasocie de las entidades de su organización según sea necesario. Dado que la política es una SCP administrada por AWS, no puede modificarla ni eliminarla. La política tiene un aspecto similar al siguiente.

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

Esta política permite a los administradores de cuentas delegar permisos para cualquier servicio o operación hasta que cree y asocie una SCP que deniegue algún acceso. Puede adjuntar una SCP que prohíba explícitamente las acciones que no desea que realicen los usuarios y roles de determinadas cuentas.

Esta política podría ser similar a la del ejemplo siguiente, que impide que los usuarios de las cuentas afectadas realicen acciones para el servicio de Amazon DynamoDB. El administrador de la organización puede desasociar la política `FullAWSAccess` y asociar esta en su lugar. Tenga en cuenta que esta SCP sigue permitiendo todos los demás servicios y sus acciones.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAllActions",
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
```

```
        },
        {
            "Sid": "DenyDynamoDB",
            "Effect": "Deny",
            "Action": "dynamodb:*",
            "Resource": "*"
        }
    ]
}
```

Los usuarios de las cuentas afectadas no pueden realizar acciones de DynamoDB porque la`Deny`en la segunda instrucción anula el elemento explícito`Allow`En la primera. Otra forma de configurar esto mismo sería dejar la política `FullAWSAccess` existente y adjuntar una segunda política que únicamente contenga la instrucción `Deny`, tal como se muestra aquí.

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

La combinación del`FullAWSAccess`de las políticas de y`Deny`Esta instrucción de la política de DynamoDB anterior que se aplica a un nodo raíz o unidad organizativa tiene el mismo efecto que una sola política que contenga ambas instrucciones. Todas las políticas que se aplican en un nivel especificado se combinan. Cada instrucción, independientemente de qué política la origine, se evalúa de acuerdo con las reglas descritas anteriormente (es decir, una instrucciónexplícito `Deny`reemplaza unexplícito`Allow`, que anula la opción predeterminadaimplícito`Deny`).

Uso de políticas SCP como lista de permitidos

Para utilizar las SCP como una lista de permitidos, debe sustituir la política SCP `FullAWSAccess` administrada por AWS por una SCP que permita de forma explícita solo los servicios y acciones que desee permitir. Al eliminar la SCP `FullAWSAccess` predeterminada, todas las acciones de todos los servicios estarán ahora denegadas implícitamente. La SCP personalizada invalida la instrucción `Deny` implícita con una instrucción `Allow` explícita para las acciones que desea permitir. Para que un permiso esté habilitado para una cuenta determinada, todas las SCP desde el nodo raíz pasando por cada unidad organizativa en la ruta directa hasta llegar a la cuenta, e incluso las asociadas a la propia cuenta, deben conceder ese permiso.

Notes

- Una`Allow`en un SCP no puede tener un`Resource`elemento con cualquier cosa excepto un`"*"`.
- Una`Allow`en un SCP no puede tener un`Condition`elemento en absoluto.

Una política de lista de permitidos como esta podría ser similar a la del ejemplo siguiente, que permite a los usuarios de la cuenta realizar operaciones de Amazon Elastic Compute Cloud (Amazon EC2) y Amazon CloudWatch, pero de ningún otro servicio. Todas las SCP de las unidades organizativas y del nodo raíz deben permitir también estos permisos explícitamente:

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

```
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*"
            ],
            "Resource": "*"
        }
    ]
}
```

Sintaxis de las políticas SCP

Las políticas de control de servicios (SCP) utilizan una sintaxis similar a la que se usa enAWS Identity and Access Management(IAM) y políticas basadas en recursos (como las políticas de bucket de Amazon S3). Para obtener más información acerca de las políticas de IAM y su sintaxis, consulteInformación general sobre las políticas de IAMen laGuía del usuario de IAM.

Una política SCP es un archivo de texto sin formato estructurado de acuerdo con las reglas JSON. Utiliza los elementos que se describen en este tema.

> Note
>
> Todos los caracteres de la SCP se contabilizan para calcular su tamaño máximo (p. 330). Los ejemplos que aparecen en esta guía muestran los SCP formateados con espacios en blanco adicionales para mejorar su legibilidad. Sin embargo, para ahorrar espacio si el tamaño de la política se aproxima al tamaño máximo, puede eliminar todos los espacios en blanco, como espacios y saltos de línea, que estén fuera de las comillas.

Para obtener información general sobre las SCP, consulte Políticas de control de servicios (p. 108).

Resumen de elementos

En la tabla siguiente se resumen los elementos de política que se pueden usar en las SCP. Algunos elementos de política solo están disponibles en las SCP que deniegan acciones. LaEfectos admitidosLa columna enumera el tipo de efecto que puede utilizar con cada elemento de política de en las SCP.

Elemento	Finalidad	Efectos admitidos
Versión (p. 126)	Especifica las reglas de sintaxis del lenguaje que se utilizarán para procesar la política.	`Allow`, `Deny`
Statement (p. 126)	Sirve como contenedor de elementos de política. Una SCP puede contener varias instrucciones.	`Allow`, `Deny`

Elemento	Finalidad	Efectos admitidos
Statement ID (Sid) (ID de instrucción) (p. 126)	(Opcional) Proporciona un nombre fácil de recordar para la instrucción.	`Allow`, `Deny`
Efecto (p. 127)	Define si la instrucción SCPPermite (p. 8)orniega (p. 8)acceso a los usuarios y roles de IAM en una cuenta.	`Allow`, `Deny`
Acción (p. 128)	Especifica.AWSEl servicio y las acciones de que la SCP permite o deniega.	`Allow`, `Deny`
NotAction (p. 128)	Especifica.AWSServicios y acciones que quedan exentos de la SCP. Se utiliza en lugar del elemento `Action`.	`Deny`
Recurso (p. 129)	Especifica los recursos de AWS a los que se aplica la SCP.	`Deny`
Condición (p. 130)	Especifica las condiciones que determinan cuándo se aplica la instrucción.	`Deny`

En las secciones siguientes se proporcionan más información y ejemplos sobre cómo usar los elementos de política en las SCP.

`Version`ELEMENT

Todas las SCP deben incluir un elemento `Version` con el valor `"2012-10-17"`. Este es el mismo valor de versión que la versión más reciente de las políticas de permisos de IAM.

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

Para obtener más información, consulteElementos de política JSON de: Versionen laGuía del usuario de IAM.

`Statement`ELEMENT

Una política SCP consta de uno o varios elementos `Statement`. Solo puede tener una palabra clave `Statement` en una política, pero el valor puede ser una matriz de instrucciones JSON (rodeadas por caracteres [ ]).

En el siguiente ejemplo se muestra una única instrucción que consta de`Effect`,`Action`, y`Resource`Elementos.

```
    "Statement": {
        "Effect": "Allow",
        "Action": "*",
        "Resource": "*"
    }
```

El siguiente ejemplo incluye dos instrucciones como una lista de matriz dentro de un elemento `Statement`. La primera instrucción permite todas las acciones, mientras que la segunda deniega todas las acciones de EC2. El resultado es que un administrador de la cuenta puede delegar cualquier permisoExceptoLas de Amazon Elastic Compute Cloud (Amazon EC2).

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "ec2:*",
            "Resource": "*"
        }
    ]
```

Para obtener más información, consulteElementos de política JSON de: Instrucciónen laGuía del usuario de IAM.

Elemento de ID de instrucción (`Sid`)

El elemento `Sid` es un identificador opcional que se proporciona para la instrucción de la política. Puede asignar un valor de `Sid` a cada instrucción de una matriz de instrucciones. En el siguiente ejemplo de SCP se incluye una instrucción `Sid` de muestra.

```
{
    "Statement": {
        "Sid": "AllowsAllActions",
        "Effect": "Allow",
        "Action": "*",
        "Resource": "*"
```

```
    }
}
```

Para obtener más información, consulteElementos de política JSON de: Iden laGuía del usuario de IAM.

`Effect`ELEMENT

Cada instrucción debe contener un elemento `Effect`. El valor puede ser `Allow` o `Deny`. Afecta a las acciones enumeradas en la misma instrucción.

Para obtener más información, consulteElementos de política JSON de: Efectoen laGuía del usuario de IAM.

`"Effect": "Allow"`

En el siguiente ejemplo se muestra una SCP con una instrucción que contiene una`Effect`elemento con un valor de`Allow`que permite a los usuarios de la cuenta realizar acciones para el servicio Amazon S3. Este ejemplo es útil en una organización que utiliza elEstrategia de lista permitida (p. 8)(donde el valor predeterminado`FullAWSAccess`Para que los permisos se deniegan implícitamente de forma predeterminada). El resultado es que la declaraciónPermite (p. 8)Los permisos de Amazon S3 para cualquier cuenta asociada:

```
{
    "Statement": {
        "Effect": "Allow",
        "Action": "s3:*",
        "Resource": "*"
    }
}
```

A pesar de que esta declaración utiliza el mismo`Allow`como política de permisos de IAM, en una SCP no concede en realidad permiso de usuario de para hacer nada. En su lugar, los SCPs actúan comofiltersque especifican los permisos máximos para las cuentas de una organización, unidad organizativa (OU) o cuenta. En el ejemplo anterior, aunque un usuario de la cuenta tuviera la`AdministratorAccess`directiva administrada adjunta, este SCP limitaTodoen las cuentas afectadas solo las acciones de Amazon S3.

`"Effect": "Deny"`

En una instrucción cuyo elemento `Effect` tiene el valor `Deny`, también puede restringir el acceso a recursos específicos o definir condiciones que determinen cuándo se aplicará la SCP.

A continuación, se muestra un ejemplo de cómo utilizar una clave de condición en una instrucción de denegación.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": "ec2:RunInstances",
        "Resource": "arn:aws:ec2:*:*:instance/*",
        "Condition": {
            "StringNotEquals": {
                "ec2:InstanceType": "t2.micro"
            }
        }
    }
}
```

Esta instrucción de una SCP establece una medida de seguridad para evitar que las cuentas afectadas (cuando la SCP se adjunte a la propia cuenta o al nodo raíz de la organización o unidad organizativa

que contiene la cuenta) lancen instancias de Amazon EC2 si estas instancias de Amazon EC2 no están establecidas en`t2.micro`. Aunque se adjunte a la cuenta una política de IAM que permita esta acción, la medida de seguridad creada por la SCP la impedirá.

`Action`y`NotAction`Elementos

Cada instrucción debe contener uno de los elementos siguientes:

- En las instrucciones de permiso o denegación, un elemento `Action`.
- En las instrucciones de denegación solo (cuando el valor del elemento `Effect` sea `Deny`), un elemento `Action` o `NotAction`.

El valor del elemento `Action` o `NotAction` es una lista (una matriz JSON) de cadenas que identifican los servicios y acciones de AWS que la instrucción permite o deniega.

Cada cadena consta de la abreviatura del servicio (como "s3", "ec2", "iam" u "organizaciones"), en letras minúsculas, seguida de un carácter de punto y coma y una acción de ese servicio. Las acciones e inacciones distinguen entre mayúsculas y minúsculas, y deben especificarse tal y como aparecen en la documentación de cada servicio. Por lo general, todas deben especificarse con cada palabra con la inicial en mayúsculas y el resto en minúsculas. Por ejemplo: `"s3:ListAllMyBuckets"`.

También puede utilizar un asterisco como comodín para que coincida con varias acciones que comparten parte de un nombre. El valor`"s3:*"`significa todas las acciones del servicio Amazon S3. El valor `"ec2:Describe*"` coincide solo con las acciones de EC2 que empiezan por "Describe".

> **Note**
>
> En una política SCP, el carácter comodín (*) de un elemento `Action` o `NotAction` únicamente puede aparecer solo o al final de la cadena. No puede aparecer al principio o en el medio de la cadena. Por lo tanto, `"servicename:action*"` es válido, pero `"servicename:*action"` y `"servicename:some*action"` no son válidos en las políticas SCP.

Para obtener una lista de todos los servicios y las acciones que se admiten tanto enAWS Organizationsdirectivas de permisos de SCPs e IAM, consulteAcciones, recursos y claves de condiciones deAWSServiciosen laGuía del usuario de IAM.

Para obtener más información, consulteElementos de política JSON de: AcciónyElementos de política JSON de: NotActionen laGuía del usuario de IAM.

Ejemplo de elemento `Action`

El siguiente ejemplo muestra una política SCP con una instrucción que permite a los administradores de la cuenta delegar los permisos describe, start, stop y terminate para las instancias EC2 de la cuenta. Se trata de otro ejemplo de una política de lista de permitidos (p. 8) y es útil cuando las políticas `Allow *` predeterminadas no están asociadas y, por tanto, los permisos se deniegan implícitamente de forma predeterminada. Si la opción predeterminada`Allow *`Esta política sigue estando asociada a la raíz, unidad organizativa o cuenta a la que la siguiente política está asociada, la política no tiene ningún efecto.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
          "ec2:DescribeInstances", "ec2:DescribeImages", "ec2:DescribeKeyPairs",
          "ec2:DescribeSecurityGroups", "ec2:DescribeAvailabilityZones",
 "ec2:RunInstances",
          "ec2:TerminateInstances", "ec2:StopInstances", "ec2:StartInstances"
        ],
        "Resource": "*"
```

```
    }
}
```

El siguiente ejemplo muestra cómo puede denegar el acceso (p. 8) a servicios que no desea usar en cuentas asociadas. Se asume que las políticas SCP `"Allow *"` predeterminadas siguen estando asociadas a las unidades organizativas y al nodo raíz. Esta política de ejemplo impide que los administradores de las cuentas asociadas deleguen permisos para los servicios de IAM, Amazon EC2 y Amazon RDS. Cualquier acción desde otros servicios se puede delegar siempre y cuando no exista otra política asociada que la deniegue.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": [ "iam:*", "ec2:*", "rds:*" ],
        "Resource": "*"
    }
}
```

Ejemplo de elemento `NotAction`

En el ejemplo siguiente se muestra cómo puede utilizar un elemento `NotAction` para excluir servicios de AWS del efecto de la política.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LimitActionsInRegion",
      "Effect": "Deny",
      "NotAction": "iam:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "us-west-1"
        }
       }
     }
   ]
}
```

Con esta instrucción, las cuentas afectadas se limitan a realizar acciones de en la Región de AWS , excepto cuando se usan acciones de IAM.

`Resource`ELEMENT

En las instrucciones cuyo elemento `Effect` tiene el valor `Allow`, puede especificar solamente "*" en el elemento `Resource` de una SCP. No puede especificar los nombres de recurso de Amazon (ARN) de los recursos individuales.

En las instrucciones cuyo elemento `Effect` tiene el valor `Deny`, puede especificar ARN individuales, como se muestra en el ejemplo siguiente.

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

```
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/role-to-deny"
      ]
    }
  ]
}
```

Esta SCP restringe a los usuarios y roles de IAM de las cuentas afectadas para que no puedan realizar cambios en un rol de IAM de administrativo común creado en todas las cuentas de la organización.

Para obtener más información, consulteElementos de política JSON de: Recursoen laGuía del usuario de IAM.

`Condition`ELEMENT

Puede especificar un elemento `Condition` en las instrucciones de denegación de una SCP.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "cloudfront:*",
                "iam:*",
                "route53:*",
                "support:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
                }
            }
        }
    ]
}
```

Esta SCP deniega el acceso a todas las operaciones fuera de las regiones `eu-central-1` y `eu-west-1`, excepto para las acciones de los servicios enumerados.

Para obtener más información, consulteElementos de política JSON de: Condiciónen laGuía del usuario de IAM.

Elementos no compatibles

Los siguientes elementos no son compatibles con las SCP:

- `Principal`
- `NotPrincipal`
- `NotResource`

Ejemplo de políticas de control de servicios

Los ejemplos de políticas de control de servicios (SCP) (p. 108) que se muestran en este tema solo tienen fines informativos.

Antes de usar estos ejemplos

Antes de utilizar estos ejemplos de SCP de en la organización, haga lo siguiente:

- Revise atentamente y personalícese las SCP según sus requisitos únicos.
- Pruebe a fondo los SCPs en su entorno con elAWSLos servicios de que utilice.

  Las políticas de ejemplo de esta sección demuestran la implementación y el uso de SCP. Ellos sonnodestinados a ser interpretados como oficialesAWSrecomendaciones o prácticas óptimas que se apliquen exactamente como se indica. Es su responsabilidad probar cuidadosamente cualquier política basada en denegaciones para determinar su idoneidad para resolver los requisitos empresariales de su entorno. Las políticas de control de servicios basadas en denegación pueden limitar o bloquear involuntariamente el uso deAWSa menos que agregue las excepciones necesarias a la directiva. Para ver un ejemplo de tal excepción, vea el primer ejemplo que exime a los servicios globales de las reglas que bloquean el acceso a Regiones de AWS .
- Recuerde que un SCP afecta a todos los usuarios y rolesen todas las cuentas a las que se adjunta.

Tip

Puede usarLos datos del último acceso al servicioinIAMPara actualizar las SCP para restringir el acceso a solo lasAWSlos servicios que necesita. Para obtener más información, consulteVisualización de los datos del último acceso al servicio de Organizationsen laGuía del usuario de IAM.

Cada una de las siguientes políticas es un ejemplo de una estrategia de política de lista de denegación (p. 122) . Las políticas de lista de denegación deben adjuntarse junto con otras políticas que permitan las acciones aprobadas en las cuentas afectadas. Por ejemplo, la política `FullAWSAccess` predeterminada permite el uso de todos los servicios de una cuenta. Esta política se adjunta de forma predeterminada a la raíz, a todas las unidades organizativas (OU) y a todas las cuentas. En realidad no concede los permisos; ninguna SCP lo hace. En su lugar, permite a los administradores de la cuenta delegar el acceso a esas acciones adjuntandoAWS Identity and Access Management(IAM) a usuarios, roles o grupos de la cuenta. Cada una de estas políticas de lista de denegación sustituye cualquier política mediante el bloqueo del acceso a los servicios o acciones especificados.

Ejemplos

- Ejemplos generales (p. 132)
  - Denegar acceso aAWSbasado en la solicitud Región de AWS (p. 132)
  - Evitar que los usuarios y las funciones de IAM realicen determinados cambios (p. 134)
  - Impedir que los usuarios y roles de IAM realicen cambios especificados, con una excepción para un rol de administrador especificado (p. 134)
  - Requerir a MFA para realizar una acción de API (p. 135)
  - Bloquear el acceso al servicio para el usuario raíz (p. 135)
  - Evitar que las cuentas miembro dejen la organización (p. 136)

Ejemplos generales

Denegar acceso aAWSbasado en la solicitud Región de AWS

Este SCP deniega el acceso a cualquier operación fuera de las regiones especificadas. Reemplazar`eu-central-1`y`eu-west-1`con Regiones de AWS que desea usar. Proporciona exenciones para operaciones en servicios globales aprobados. En este ejemplo también se muestra cómo exonerar las solicitudes realizadas por cualquiera de las dos funciones de administrador especificadas.

> **Important**
>
> Si usaAWS Control TowerEn la organización, le recomendamos que no utilice esta política de ejemplo.AWS Control Towerfunciona en Regiones de AWS de una manera que no sea compatible con esta política de ejemplo.

Esta política utiliza el efecto `Deny` para denegar el acceso a todas las solicitudes de operaciones que no se encuentran en una de las dos regiones aprobadas (`eu-central-1` y `eu-west-1`). El elemento NotAction permite enumerar los servicios cuyas operaciones (u operaciones individuales) están exentas de esta restricción. Dado que los servicios globales tienen puntos de enlace alojados físicamente por la`us-east-1`En la región, deben quedar exentos de esta manera. Con un SCP estructurado de esta manera, se permiten las solicitudes hechas a servicios globales en la región `us-east-1` si el servicio solicitado está incluido en el elemento `NotAction`. Cualquier otra solicitud a los servicios de la región `us-east-1` se deniega mediante esta política de ejemplo.

> **Note**
>
> Este ejemplo puede no incluir todos losAWSservicios u operaciones. Sustituya la lista de servicios y operaciones por los servicios globales que las cuentas de la organización utilizan.
>
> > **Tip**
> >
> > Puede ver laLos datos del último acceso a los servicios en la consola de IAMPara determinar qué servicios globales utiliza la organización. LaAcceso a AdvisorEn la página

de detalles de un usuario, grupo o rol de IAM se muestra laAWSLos servicios que ha utilizado esa entidad, ordenados por el acceso más reciente.

Considerations

- AWS KMSyAWS Certificate Manageradmiten puntos finales regionales. Sin embargo, si desea utilizarlos con un servicio global como Amazon CloudFront, debe incluirlos en la lista de exclusión de servicios globales del siguiente ejemplo SCP. Un servicio global comoAWS CloudFormationnormalmente requiere acceso aAWS KMSy ACM en la misma región, que para un servicio global es la región EE. UU. Este (Norte de Virginia) (`us-east-1`).
- De forma predeterminada,AWS STSes un servicio global y debe incluirse en la lista de exclusión de servicios globales. Sin embargo, puede habilitarAWS STSPara utilizar los puntos finales de región en lugar de un único punto de enlace global. Si lo hace, puede eliminar STS de la lista de exención de servicio global en el siguiente ejemplo SCP. Para obtener más información, consulteAdministraciónAWS STSen un Región de AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "a4b:*",
                "acm:*",
                "aws-marketplace-management:*",
                "aws-marketplace:*",
                "aws-portal:*",
                "budgets:*",
                "ce:*",
                "chime:*",
                "cloudfront:*",
                "config:*",
                "cur:*",
                "directconnect:*",
                "ec2:DescribeRegions",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeVpnGateways",
                "fms:*",
                "globalaccelerator:*",
                "health:*",
                "iam:*",
                "importexport:*",
                "kms:*",
                "mobileanalytics:*",
                "networkmanager:*",
                "organizations:*",
                "pricing:*",
                "route53:*",
                "route53domains:*",
                "s3:GetAccountPublic*",
                "s3:ListAllMyBuckets",
                "s3:PutAccountPublic*",
                "shield:*",
                "sts:*",
                "support:*",
                "trustedadvisor:*",
                "waf-regional:*",
                "waf:*",
                "wafv2:*",
                "wellarchitected:*"
            ],
```

```
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

Evitar que los usuarios y las funciones de IAM realicen determinados cambios

Esta SCP restringe a los usuarios y roles de IAM para que no puedan realizar cambios en el rol de IAM especificado que creó en todas las cuentas de la organización.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessToASpecificRole",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/name-of-role-to-deny"
      ]
    }
  ]
}
```

Impedir que los usuarios y roles de IAM realicen cambios especificados, con una excepción para un rol de administrador especificado

Esta SCP se basa en el ejemplo anterior, pero especifica una excepción para los administradores. Impide que los usuarios y roles de IAM de las cuentas afectadas realicen cambios en un rol de IAM de administrativo común creado en todas las cuentas de la organizaciónExceptopara los administradores que utilizan un rol especificado.

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

```
      "Sid": "DenyAccessWithException",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/name-of-role-to-deny"
      ],
      "Condition": {
        "StringNotLike": {
          "aws:PrincipalARN":"arn:aws:iam::*:role/name-of-admin-role-to-allow"
        }
      }
    }
  ]
}
```

Requerir a MFA para realizar una acción de API

Utilice una SCP similar a la siguiente para requerir que la autenticación multifactor (MFA) esté habilitada para que un usuario o función de IAM pueda realizar una acción. En este ejemplo, la acción consiste en detener una instancia Amazon EC2.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyStopAndTerminateWhenMFAIsNotPresent",
      "Effect": "Deny",
      "Action": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*",
      "Condition": {"BoolIfExists": {"aws:MultiFactorAuthPresent": false}}
    }
  ]
}
```

Bloquear el acceso al servicio para el usuario raíz

La siguiente política restringe todo acceso a las acciones especificadas para laUsuario raízen una cuenta miembro. Si desea evitar que en sus cuentas se usen las credenciales raíz de determinadas maneras concretas, añada sus propias acciones a esta política.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RestrictEC2ForRoot",
      "Effect": "Deny",
      "Action": [
        "ec2:*"
```

```
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::*:root"
          ]
        }
      }
    }
  ]
}
```

Evitar que las cuentas miembro dejen la organización

La siguiente directiva impide que los administradores de cuentas miembros eliminen sus cuentas de la organización bloqueando el uso de la`LeaveOrganization`Operación API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "organizations:LeaveOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

Ejemplo de SCP para Amazon CloudWatch

Ejemplos en esta categoría

- Evitar que los usuarios deshabiliten CloudWatch o modifiquen su configuración (p. 136)

Evitar que los usuarios deshabiliten CloudWatch o modifiquen su configuración

Un operador de CloudWatch de nivel inferior necesita monitorear tableros y alarmas. Sin embargo, el operador no debe poder eliminar ni cambiar ningún panel o alarma que puedan haber aplicado las personas mayores. Esta SCP evita que los usuarios o roles de cualquier cuenta afectada ejecuten cualquiera de los comandos de CloudWatch que podrían eliminar o cambiar sus paneles o alarmas.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DeleteDashboards",
        "cloudwatch:DisableAlarmActions",
        "cloudwatch:PutDashboard",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:SetAlarmState"
      ],
      "Resource": "*"
```

```
    }
  ]
}
```

SCP de ejemplo paraAWS Config

Ejemplos en esta categoría

- Impedir que los usuarios desactivenAWS Configo cambiar sus reglas (p. 137)

Impedir que los usuarios desactivenAWS Configo cambiar sus reglas

Esta SCP evita que los usuarios o las funciones de cualquier cuenta afectada ejecuten operaciones de AWS Config que podrían deshabilitar AWS Config o modificar sus reglas o disparadores.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "config:DeleteConfigRule",
        "config:DeleteConfigurationRecorder",
        "config:DeleteDeliveryChannel",
        "config:StopConfigurationRecorder"
      ],
      "Resource": "*"
    }
  ]
}
```

Ejemplo de SCP para Amazon Elastic Compute Cloud (Amazon EC2)

Ejemplos en esta categoría

- Requerir que las instancias Amazon EC2 utilicen un tipo específico (p. 137)

Requerir que las instancias Amazon EC2 utilicen un tipo específico

Con esta SCP, se denegarán todos los lanzamientos de instancias qeu no usen el tipo de instancia `t2.micro`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RequireMicroInstanceType",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ec2:InstanceType": "t2.micro"
        }
      }
    }
```

```
  ]
}
```

Ejemplo de SCP para Amazon GuardDuty

Ejemplos en esta categoría

- Evitar que los usuarios deshabiliten GuardDuty o modifiquen su configuración (p. 138)

Evitar que los usuarios deshabiliten GuardDuty o modifiquen su configuración

Esta SCP evita que los usuarios o roles de cualquier cuenta afectada deshabiliten GuardDuty o modifiquen su configuración, ya sea directamente como un comando o a través de la consola. Permite el acceso de solo lectura a la GuardDuty los recursos de.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "guardduty:AcceptInvitation",
                "guardduty:ArchiveFindings",
                "guardduty:CreateDetector",
                "guardduty:CreateFilter",
                "guardduty:CreateIPSet",
                "guardduty:CreateMembers",
                "guardduty:CreatePublishingDestination",
                "guardduty:CreateSampleFindings",
                "guardduty:CreateThreatIntelSet",
                "guardduty:DeclineInvitations",
                "guardduty:DeleteDetector",
                "guardduty:DeleteFilter",
                "guardduty:DeleteInvitations",
                "guardduty:DeleteIPSet",
                "guardduty:DeleteMembers",
                "guardduty:DeletePublishingDestination",
                "guardduty:DeleteThreatIntelSet",
                "guardduty:DisassociateFromMasterAccount",
                "guardduty:DisassociateMembers",
                "guardduty:InviteMembers",
                "guardduty:StartMonitoringMembers",
                "guardduty:StopMonitoringMembers",
                "guardduty:TagResource",
                "guardduty:UnarchiveFindings",
                "guardduty:UntagResource",
                "guardduty:UpdateDetector",
                "guardduty:UpdateFilter",
                "guardduty:UpdateFindingsFeedback",
                "guardduty:UpdateIPSet",
                "guardduty:UpdatePublishingDestination",
                "guardduty:UpdateThreatIntelSet"
            ],
            "Resource": "*"
        }
    ]
}
```

SCP de ejemplo paraAWS Resource Access Manager

Ejemplos en esta categoría

Impedir compartir externamente

El siguiente ejemplo SCP impide que los usuarios creen recursos compartidos que permiten compartir con usuarios de IAM y roles que no forman parte de la organización.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:CreateResourceShare",
                "ram:UpdateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "ram:RequestedAllowsExternalPrincipals": "true"
                }
            }
        }
    ]
}
```

Permitir que determinadas cuentas compartan solo tipos de recursos especificados

El siguiente SCP permite cuentas`111111111111`y`222222222222`para crear recursos compartidos que compartan listas de prefijos y asociar listas de prefijos con recursos compartidos existentes.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "OnlyNamedAccountsCanSharePrefixLists",
            "Effect": "Deny",
            "Action": [
                "ram:AssociateResourceShare",
                "ram:CreateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalAccount": [
                        "111111111111",
                        "222222222222"
                    ]
                },
                "StringEquals": {
                    "ram:RequestedResourceType": "ec2:PrefixList"
                }
            }
        }
    ]
```

```
}
```

Evitar el uso compartido de organizaciones o unidades organizativas

El siguiente SCP impide que los usuarios creen recursos compartidos que comparten recursos con unAWSOrganización u OU.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:CreateResourceShare",
                "ram:AssociateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringLike": {
                    "ram:Principal": [
                        "arn:aws:organizations::*:organization/*",
                        "arn:aws:organizations::*:ou/*"
                    ]
                }
            }
        }
    ]
}
```

Permitir el uso compartido solo con usuarios y roles de IAM especificados

El siguiente ejemplo SCP permite a los usuarios compartir recursos conSoloorganizacióno-12345abcdef, unidad organizativaou-98765fedcbaCuenta, y cuenta111111111111.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:AssociateResourceShare",
                "ram:CreateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "ram:Principal": [
                        "arn:aws:organizations::123456789012:organization/o-12345abcdef",
                        "arn:aws:organizations::123456789012:ou/o-12345abcdef/
ou-98765fedcba",
                        "111111111111"
                    ]
                }
            }
        }
    ]
}
```

Ejemplo de SCPs para etiquetar recursos

Ejemplos en esta categoría

- Requerir una etiqueta en los recursos creados especificados (p. 141)
- Impedir que las etiquetas se modifiquen excepto por entidades autorizadas (p. 142)

Requerir una etiqueta en los recursos creados especificados

El siguiente SCP impide que los usuarios y roles de IAM en las cuentas afectadas creen ciertos tipos de recursos si la solicitud no incluye las etiquetas especificadas.

> **Important**
>
> Recuerde probar las políticas basadas en denegación con los servicios que utiliza en su entorno. El siguiente ejemplo es un simple bloque de creación de secretos sin etiquetar o ejecución de instancias de Amazon EC2 sin etiquetar, y no incluye ninguna excepción.
> La siguiente política de ejemplo no es compatible conAWS CloudFormationcomo está escrito, porque ese servicio crea un secreto y luego lo etiqueta como dos pasos separados. Esta política de ejemplo bloquea eficazmenteAWS CloudFormationcrear un secreto como parte de una pila, porque tal acción resultaría, aunque brevemente, en un secreto que no está etiquetado como sea necesario.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyCreateSecretWithNoProjectTag",
      "Effect": "Deny",
      "Action": "secretsmanager:CreateSecret",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:RequestTag/Project": "true"
        }
      }
    },
    {
      "Sid": "DenyRunInstanceWithNoProjectTag",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/Project": "true"
        }
      }
    },
    {
      "Sid": "DenyCreateSecretWithNoCostCenterTag",
      "Effect": "Deny",
      "Action": "secretsmanager:CreateSecret",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:RequestTag/CostCenter": "true"
        }
      }
    },
    {
      "Sid": "DenyRunInstanceWithNoCostCenterTag",
      "Effect": "Deny",
```

```
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/CostCenter": "true"
        }
      }
    }
  ]
}
```

Para obtener una lista de todos los servicios y las acciones que se admiten tanto enAWS Organizationsdirectivas de permisos de SCPs e IAM, consulteAcciones, recursos y claves de condiciones deAWSServiciosen laGuía del usuario de IAM.

Impedir que las etiquetas se modifiquen excepto por entidades autorizadas

El siguiente SCP muestra cómo una política puede permitir que sólo los principales autorizados modifiquen las etiquetas adjuntas a los recursos. Esto es una parte importante de usar el control de acceso basado en atributos (ABAC) como parte de laAWSEstrategia de seguridad en la nube. La política permite al autor de la llamada modificar las etiquetas sólo en aquellos recursos donde la etiqueta de autorización (en este ejemplo,`access-project`) coincide con la misma etiqueta de autorización asociada al usuario o rol de que realiza la solicitud. La directiva también impide que el usuario autorizado cambie elvaluede la etiqueta que se utiliza para la autorización. El principal de llamada debe tener la etiqueta de autorización para realizar cualquier cambio.

Esta directiva sólo impide que los usuarios no autorizados cambien las etiquetas. Un usuario autorizado que no esté bloqueado por esta política debe seguir teniendo una directiva de IAM independiente que otorgue explícitamente el`Allow`en las API de etiquetado pertinentes. Por ejemplo, si el usuario tiene una directiva de administrador con`Allow */*`(permitir todos los servicios y todas las operaciones), entonces la combinación da como resultado que el usuario administrador pueda cambiarSoloaquellas etiquetas que tienen un valor de etiqueta de autorización que coincide con el valor de etiqueta de autorización adjunto al principal del usuario. Esto se debe a que el`Deny`en esta política anula el`Allow`en la directiva de administrador.

> **Important**
>
> Esta no es una solución de política completa y no debe usarse como se muestra aquí. Este ejemplo sólo pretende ilustrar parte de una estrategia ABAC y debe personalizarse y probarse para entornos de producción.
> Para obtener la política completa con un análisis detallado de cómo funciona, consulteProteger las etiquetas de recursos utilizadas para la autorización mediante una directiva de control de servicios enAWS Organizations
> Recuerde probar las políticas basadas en denegación con los servicios que utiliza en su entorno.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
```

```
            ],
            "Condition": {
                "StringNotEquals": {
                    "ec2:ResourceTag/access-project": "${aws:PrincipalTag/access-project}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "Null": {
                    "ec2:ResourceTag/access-project": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/access-project": "${aws:PrincipalTag/access-project}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "access-project"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "Null": {
                    "aws:PrincipalTag/access-project": true
                }
            }
        }
    ]
}
```

Ejemplo de SCP para Amazon Virtual Private Cloud (Amazon VPC)

Ejemplos en esta categoría

- Impedir que los usuarios eliminen los registros de flujo de Amazon VPC (p. 144)

- Evitar que cualquier VPC que no tenga acceso a Internet lo obtenga (p. 144)

Impedir que los usuarios eliminen los registros de flujo de Amazon VPC

Esta SCP evita que los usuarios o roles de cualquier cuenta afectada eliminen los logs de flujo de Amazon Elastic Compute Cloud (Amazon EC2) o los grupos o secuencias de logs de CloudWatch.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:DeleteFlowLogs",
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream"
      ],
      "Resource": "*"
    }
  ]
 }
```

Evitar que cualquier VPC que no tenga acceso a Internet lo obtenga

Esta SCP evita que los usuarios o roles de cualquier cuenta afectada cambien la configuración de sus nubes virtuales privadas (VPC) de Amazon EC2 para concederles acceso directo a Internet. No bloquea el acceso directo existente ni ningún acceso que se direccione a través de su entorno de red local.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:AttachInternetGateway",
        "ec2:CreateInternetGateway",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateVpcPeeringConnection",
        "ec2:AcceptVpcPeeringConnection",
        "globalaccelerator:Create*",
        "globalaccelerator:Update*"
      ],
      "Resource": "*"
    }
  ]
}
```

Políticas de exclusión de servicios de IA

Para obtener información y procedimientos comunes a todos los tipos de políticas, consulte los siguientes temas:

- Habilitar y desactivar tipos de políticas (p. 87)
- Obtenga detalles sobre las políticas (p. 90)
- Sintaxis y herencia de políticas (p. 95)

CiertosAWSLos servicios de inteligencia artificial (IA), incluidos Amazon CodeGuru Profiler, Amazon Comprehend, Amazon Lex, Amazon Polly, Amazon Rekognition, Amazon Textract, Amazon Transcribe y Amazon Translate, pueden almacenar y utilizar el contenido del cliente procesado por dichos servicios para el desarrollo y la mejora continua de Servicios y tecnologías de IA de Amazon. ComoAWS, puede optar por no tener su contenido almacenado o utilizado para mejorar el servicio. En lugar de configurar esta configuración individualmente para cada Cuenta de AWS que utiliza su organización, puede configurar una directiva de organización que aplique la opción de configuración en todas las cuentas que sean miembros de la organización. Puede optar por no participar en el almacenamiento de contenido y utilizarlo para un servicio de IA individual, o para todos los servicios cubiertos a la vez. Puede consultar la política efectiva aplicable a cada cuenta para ver los efectos de las opciones de configuración.

Important

- Cuando especifica una preferencia de opción o exclusión para un servicio, esa configuración es global y se aplica a todos los Regiones de AWS . Establecer el valor desde dentro de uno Región de AWS Se replica a todas las demás regiones.
- Cuando se opta por no utilizar el contenido por parte de unAWSAI, ese servicio elimina todo el contenido histórico asociado que se compartió conAWSantes de establecer la opción.

Introducción a las políticas de exclusión de servicios de IA

Siga estos pasos para empezar a utilizar las políticas de exclusión de los servicios de Inteligencia Artificial (AI).

1. Habilitar políticas de exclusión de servicios de IA para su organización (p. 87).
2. Crear una política de exclusión de servicios de IA (p. 145).
3. Asocie la política de exclusión de servicios de IA a la raíz, unidad organizativa o cuenta de su organización (p. 151).
4. Consulte la política de exclusión en vigor combinada de servicios de IA que se aplica a una cuenta (p. 154).

Para todos estos pasos, debe iniciar sesión comoAWS Identity and Access ManagementInicie sesión como usuario de IAM (IAM), asuma un rol de IAM o inicie sesión como el usuario raíz (No recomendado) en la cuenta de gestión de la organización.

Información adicional

- Conozca la sintaxis de políticas para las políticas de exclusión de servicios de IA y vea ejemplos de políticas (p. 156)

Creación, actualización y eliminación de políticas de exclusión de los servicios de IA

En este tema:

- Después de tihabilitar políticas de exclusión del servicio de IA (p. 87)para su organización, puedeCrear una política (p. 146).
- Cuando cambien sus requisitos de exclusión, puedePara actualizar una política existente (p. 147).
- Cuando ya no necesite una política y después de desasociarla de todas las unidades organizativas (OU) y cuentas, puedeeliminarlo (p. 150).

Creación de una política de exclusión de servicios de IA

Permisos mínimos

Para crear una política de exclusión de servicios de IA, necesita permiso para ejecutar la siguiente acción:

- `organizations:CreatePolicy`

AWS Management Console

Para crear una política de exclusión de servicios de IA

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaPolíticas de exclusión de servicios de IAElija, elijaCrear política.
3. En la páginaCrear una nueva política de exclusión de servicios de IApageintroduzca unNombre de la políticay unDescripción de la política.
4. (Opcional) Puede agregar una o varias etiquetas a la política seleccionandoAñadir etiquetaA continuación, introduzca una clave y un valor opcional. Dejar el valor en blanco lo establece en una cadena vacía; no es`null`. Puede adjuntar hasta 50 etiquetas a una política. Para obtener más información, consulte Etiquetado de recursos de AWS Organizations (p. 229).
5. Escriba o pegue el texto de la directiva en el cuadroJSONTabulador. Para obtener información acerca de la sintaxis de las políticas de exclusión de los servicios de IA, consulteSintaxis y ejemplos de políticas de exclusión de servicios de IA (p. 156). Para ver las políticas de ejemplo que puede utilizar como punto de partida, consulteEjemplos de políticas de exclusión de servicios de IA (p. 158).
6. Cuando haya terminado de editar la política, elijaCrear políticaEn la esquina inferior derecha de la página.

AWS CLI & AWS SDKs

Para crear una política de exclusión de servicios de IA

Puede utilizar una de las siguientes opciones para crear una política de etiquetas:

- AWS CLI: create-policy

1. Cree una política de exclusión de servicios de IA como la siguiente y guárdela en un archivo de texto. Tenga en cuenta que»`optOut`" y "`optIn`«distinguen entre mayúsculas y min

```
{
    "services": {
        "default": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

Esta política de exclusión de servicios de IA especifica que todas las cuentas afectadas por la política se excluyen de todos los servicios de IA excepto Amazon Rekognition.

2. Importe el archivo de política JSON para crear una política nueva en la organización. En este ejemplo, el archivo JSON anterior se denominó`policy.json`.

```
$ aws organizations create-policy \
    --type AISERVICES_OPT_OUT_POLICY \
    --name "MyTestPolicy" \
    --description "My test policy" \
    --content file://policy.json
{
    "Policy": {
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":{\"@@assign\":
\"optOut\"}},\"rekognition\":{\"opt_out_policy\":{\"@@assign\":\"optIn\"}}}}",
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5"
            "Arn": "arn:aws:organizations::o-aa111bb222:policy/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Description": "My test policy",
            "Name": "MyTestPolicy",
            "Type": "AISERVICES_OPT_OUT_POLICY"
        }
    }
}
```

- AWSSDK de: CreatePolicy

Qué hacer a continuación

Cuando haya creado una política de exclusión de servicios de IA, puede hacer efectivas sus opciones de exclusión. Para hacer eso, puedesAsociar la política (p. 209)A la raíz de la organización, unidades organizativas (OU), Cuentas de AWS dentro de su organización, o una combinación de todos ellos.

Actualización de una política de exclusión de servicios de IA

Permisos mínimos

Para actualizar una política de exclusión de servicios de IA, debe tener permiso para ejecutar las siguientes acciones:

- `organizations:UpdatePolicy` con un elemento `Resource` en la misma instrucción de política que incluye el ARN de la política especificada (o "*")
- `organizations:DescribePolicy`con un`Resource`en la misma declaración de política que incluye el nombre de recurso de Amazon (ARN) de la política especificada (o «*»)

AWS Management Console

Para actualizar una política de exclusión de servicios de IA

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaPolíticas de exclusión de servicios de IAElija el nombre de la política que desea actualizar.
3. En la página de detalles de la política, elijaEdición de política.
4. Puede introducir un nuevoNombre de la política,Descripción de la políticao edite laJSONTexto de política. Para obtener información acerca de la sintaxis de las políticas de exclusión de los

servicios de IA, consulteSintaxis y ejemplos de políticas de exclusión de servicios de IA (p. 156). Para ver las políticas de ejemplo que puede utilizar como punto de partida, consulteEjemplos de políticas de exclusión de servicios de IA (p. 158).

5. Cuando haya terminado de actualizar la política, elija Save changes (Guardar cambios).

AWS CLI & AWS SDKs

Para actualizar una política

Puede utilizar uno de los comandos siguientes para actualizar una política:

- AWS CLI:update-policy

  En el siguiente ejemplo se cambia el nombre de una política de exclusión de servicios de IA.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":   ....TRUNCATED
 FOR BREVITY...   :{\"@@assign\":\"optIn\"}}}}"
    }
}
```

  En el ejemplo siguiente se agrega o cambia la descripción de una política de exclusión de servicios de IA.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":   ....TRUNCATED
 FOR BREVITY...   :{\"@@assign\":\"optIn\"}}}}"
    }
}
```

  En el siguiente ejemplo se cambia el documento de directiva JSON adjunto a una política de exclusión de servicios de IA. En este ejemplo, el contenido se toma de un archivo llamado`policy.json`Con el texto siguiente:

```
{
```

```
    "services": {
        "default": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "comprehend": {
            "opt_out_policy": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
        },
         "Content": "{\n\"services\": {\n\"default\": {\n\"   ....TRUNCATED FOR
 BREVITY....    ": \"optIn\"\n}\n}\n}\n"}
}
```

- AWSSDK de: UpdatePolicy

Edición de etiquetas adjuntas a una política de exclusión de servicios de IA

Cuando inicia sesión en la cuenta de administración de su organización, puede agregar o eliminar las etiquetas asociadas a una política de exclusión de servicios de IA. Para obtener más información acerca del etiquetado, consulte Etiquetado de recursos de AWS Organizations (p. 229).

Permisos mínimos

Para editar las etiquetas adjuntas a una política de exclusión de servicios de IA en suAWS, debe disponer de los siguientes permisos:

- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:DescribePolicy`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

Para editar las etiquetas adjuntas a una política de exclusión de servicios de IA

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaPolíticas de exclusión de servicios de IA, elija el nombre de la política con las etiquetas que desea editar.
3. En la página de detalles de la política seleccionada, elija la opciónTags (Etiquetas):Elija y, a continuación, elijaAdministrar etiquetas.
4. Puede realizar cualquiera de estas acciones en esta página:
   - Edite el valor de cualquier etiqueta introduciendo un nuevo valor sobre el anterior. No se puede modificar la clave. Para cambiar una clave, debe eliminar la etiqueta con la clave anterior y agregar una etiqueta con la nueva clave.
   - Elimine una etiqueta existente seleccionandoRemove.
   - Agregue una clave de etiqueta y un par de valor. SeleccionarAñadir etiquetay, a continuación, introduzca el nuevo nombre de clave y el valor opcional en los cuadros proporcionados. Si deja elValorEn blanco, el valor es una cadena vacía; no es`null`.
5. SeleccionarGuarde los cambiosdespués de haber realizado todas las adiciones, eliminaciones y ediciones que desee realizar.

AWS CLI & AWS SDKs

Para editar las etiquetas adjuntas a una política de exclusión de servicios de IA

Puede utilizar uno de los comandos siguientes para editar las etiquetas adjuntas a una política de exclusión de servicios de IA:

- AWS CLI:tag-resourceyuntag-resource
- AWSSDK de: TagResourceyUntagResource

Eliminación de una política de exclusión de servicios de IA

Cuando inicia sesión en la cuenta de administración de su organización, puede eliminar una política que ya no necesite en su organización.

Para poder eliminar una política, primero debe desasociarla de todas las entidades asociadas.

Permisos mínimos

Para eliminar una política, debe tener permiso para ejecutar la siguiente acción:

- `organizations:DescribePolicy`(sólo consola — para navegar a la directiva)
- `organizations:DeletePolicy`

AWS Management Console

Para eliminar una política de exclusión de servicios de IA

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaPolíticas de exclusión de servicios de IAElija el nombre de la política que desea ver.

3. Debe desasociar primero la política que desea eliminar de todas las raíces, unidades organizativas y cuentas. Elija el iconoimplementación, elija el botón de opción situado junto a cada raíz, unidad organizativa o cuenta que se muestra en la pestañaimplementaciónElija y, a continuación, elijaSeparar. En el cuadro de diálogo de confirmación, elijaSeparar. Repita la operación hasta que elimine todos los destinos.
4. SeleccionarEliminarEn la parte superior de la página.
5. En el cuadro de diálogo de confirmación, escriba el nombre de la política y, a continuación, elijaEliminar.

AWS CLI & AWS SDKs

Para eliminar una política de exclusión de servicios de IA

Puede utilizar uno de los comandos siguientes para eliminar una política:

- AWS CLI: delete-policy

  En el siguiente ejemplo se elimina la política especificada. Sólo funciona si la política no está asociada a ninguna raíz, unidad organizativa o cuenta.

```
$ aws organizations delete-policy \
    --policy-id p-i9j8k7l6m5
```

  Este comando no genera ninguna salida cuando se realiza correctamente.
- AWSSDK de: DeletePolicy

Adjuntar y separar políticas de exclusión de servicios de IA

Puede utilizar las políticas de exclusión de servicios de inteligencia artificial (IA) en toda una organización además de en las unidades organizativas (OU) y las cuentas individuales. A qué se aplica la política de exclusión de servicios de IA depende del elemento de la organización al que se adjunte:

- Al adjuntar una política de exclusión de servicios de IA a suraíz de la organización, la política se aplica a todas las cuentas y unidades organizativas de los miembros de la raíz.
- Cuando se adjunta una política de exclusión de servicios de IA a unOU, esa política se aplica a las cuentas que pertenecen a la unidad organizativa o a cualquiera de sus unidades organizativas secundarias. Esas cuentas también están sujetas a cualquier política de copia de seguridad asociada a la raíz de la organización.
- Cuando se adjunta una política de exclusión de servicios de IA a unaccount, esa política sólo se aplica a esa cuenta. La cuenta también está sujeta a cualquier política asociada a la raíz de la organización y a las unidades organizativas a las que pertenezca la cuenta.

La agregación de cualquier política de exclusión de servicios de IA que herede la cuenta de las unidades organizativas raíz y principales, así como de cualquier política directamente asociada a la cuenta, es laPolítica en vigor (p. 154). Para obtener información sobre cómo se fusionan las políticas con la política en vigor, consulte Descripción de la herencia de políticas (p. 94).

Permisos mínimos

Para asociar políticas de exclusión de servicios de IA, debe tener permiso para ejecutar la siguiente acción:

- `organizations:AttachPolicy`

AWS Management Console

Puede adjuntar una política de exclusión de servicios de IA navegando hasta la política o hasta la raíz, unidad organizativa o cuenta a la que desee adjuntar la política.

Para asociar una política de exclusión de servicios de IA, vaya al directorio raíz, unidad organizativa o cuenta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la página Cuentas de AWS , elija el nombre de la raíz, unidad organizativa o cuenta a la que desea adjuntar una política. Es posible que tenga que expandir las unidades organizativas (elija la opción▶) para encontrar la unidad organizativa o la cuenta que desea.
3. En el navegadorPolíticas, en la entrada dePolíticas de exclusión de servicios de IA, elijaAttach.
4. Busque la política que desea y elijaAsociar política.

   La lista de políticas de exclusión de los servicios de IA adjuntas en elPolíticasse actualiza para incluir la nueva adición. El cambio de política surtirá efecto de inmediato.

Para adjuntar una política de exclusión de servicios de IA navegando a la directiva

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaPolíticas de exclusión de servicios de IAElija el nombre de la política que desea adjuntar.
3. En la páginaimplementaciónElija, elijaAttach.
4. Elija el botón de opción situado junto a la raíz, unidad organizativa o cuenta a la que desee adjuntar la política. Es posible que tenga que expandir las unidades organizativas (elija la opción▶) para encontrar la unidad organizativa o la cuenta que desea.
5. Elija Attach policy (Asociar política).

   La lista de políticas de exclusión de los servicios de IA adjuntas en elimplementaciónse actualiza para incluir la nueva adición. El cambio de política surtirá efecto de inmediato.

AWS CLI & AWS SDKs

Para asociar una política de exclusión de servicios de IA a la raíz de la organización, la unidad organizativa o la cuenta

Puede utilizar uno de los comandos siguientes para asociar una política de exclusión de servicios de IA:

- AWS CLI:Asociate-policy

  En el siguiente ejemplo se adjunta una política a una unidad organizativa.

```
$ aws organizations attach-policy \
    --target-id ou-a1b2-f6g7h222 \
    --policy-id p-i9j8k7l6m5
```

  Este comando no genera ninguna salida cuando se realiza correctamente.
- AWSSDK de: AttachPolicy

El cambio de política surtirá efecto de inmediato.

Desvinculación de una política de exclusión de servicios de IA

Cuando inicia sesión en la cuenta de administración de su organización, puede desasociar una política de exclusión de servicios de IA de la raíz de la organización, unidad organizativa o cuenta a la que está asociada. Después de desasociar una política de exclusión de servicios de IA de una entidad, dicha política ya no se aplica a ninguna cuenta que estuviera afectada por la entidad ahora desasociada. Para desasociar una política, siga los pasos que se describen a continuación.

Permisos mínimos

Para desasociar una política de exclusión de servicios de IA de la raíz de la organización, unidad organizativa o cuenta, debe tener permiso para ejecutar la siguiente acción:

- `organizations:DetachPolicy`

AWS Management Console

Puede desasociar una política de exclusión de servicios de IA navegando hasta la política o hasta la raíz, unidad organizativa o cuenta de la que desea desasociar la política.

Para desasociar una política de exclusión de servicios de IA navegando hasta la raíz, unidad organizativa o cuenta a la que esté asociada

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la página Cuentas de AWS Vaya a la raíz, unidad organizativa o cuenta de la que desea desasociar una política. Es posible que tenga que expandir las unidades organizativas (elija la opción▶) para encontrar la unidad organizativa o la cuenta que desea. Elija el nombre de raíz, unidad organizativa o cuenta.
3. En la páginaPolíticas, elija el botón de opción situado junto a la política de exclusión de servicios de IA que desea desasociar y, a continuación, elijaSeparar.
4. En el cuadro de diálogo de confirmación, elijaPolítica de desvinculación.

   Se actualiza la lista de políticas de exclusión de servicios de IA adjuntas. El cambio de política surtirá efecto de inmediato.

Para separar una política de exclusión de servicios de IA navegando a la directiva

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaPolíticas de exclusión de servicios de IA, elija el nombre de la política que desea desasociar de una raíz, unidad organizativa o cuenta.
3. En la páginaimplementación, elija el botón de opción situado junto a la raíz, unidad organizativa o cuenta de la que desea desasociar la política. Es posible que tenga que expandir las unidades organizativas (elija la opción▶) para encontrar la unidad organizativa o la cuenta que desea.
4. Elija Detach (Desasociar).
5. En el cuadro de diálogo de confirmación, elijaSeparar.

   Se actualiza la lista de políticas de exclusión de servicios de IA adjuntas. El cambio de política surtirá efecto de inmediato.

AWS CLI & AWS SDKs

Para desasociar una política de exclusión de servicios de IA de la raíz de la organización, la unidad organizativa o la cuenta

Puede utilizar uno de los comandos siguientes para desasociar una política de exclusión de servicios de IA:

- AWS CLI:detach-policy

  En el ejemplo siguiente se desconecta una directiva de una unidad organizativa.

```
$ aws organizations detach-policy \
    --target-id ou-a1b2-f6g7h222 \
    --policy-id p-i9j8k7l6m5
```

  Este comando no genera ninguna salida cuando se realiza correctamente.
- AWSSDK de: DetachPolicy

El cambio de política surtirá efecto de inmediato.

Visualización de políticas efectivas de exclusión de servicios de IA

Determine la política de exclusión en vigor de servicios de inteligencia artificial (IA) para una cuenta de su organización.

¿Cuál es la política de exclusión efectiva de los servicios de IA?

Lapolítica de exclusión efectiva de servicios de IAespecifica las reglas finales que se aplican a un Cuenta de AWS . Es la agregación de cualquier política de exclusión de servicios de IA que herede la cuenta, además de cualquier política de exclusión de servicios de IA que se asocie directamente a la cuenta. Cuando asocia una política de exclusión de servicios de IA a la raíz de la organización, esta se aplica a todas las cuentas de la organización. Cuando asocia una política de exclusión de servicios de IA a una unidad organizativa, esta se aplica a todas las cuentas y unidades organizativas que pertenecen a la unidad organizativa. Cuando asocia una política directamente a una cuenta, solo se aplica a esa cuenta. Cuenta de AWS .

Por ejemplo, la política de exclusión de servicios de IA asociada a la raíz de la organización puede especificar que todas las cuentas de la organización no utilicen contenido de todas las cuentas deAWSServicios de aprendizaje automático. Una política de exclusión independiente de servicios de IA adjunta directamente a una cuenta de miembro especifica que opta por el uso de contenido solo para Amazon Rekognition. La combinación de estas políticas de exclusión de servicios de IA incluye la política de exclusión efectiva de servicios de IA. El resultado es que todas las cuentas de la organización están excluidas de todas lasAWS, con la excepción de una cuenta que opte por Amazon Rekognition.

Para obtener información acerca de cómo se combinan las políticas en la política en vigor final, consulteDescripción de la herencia de políticas (p. 94).

Cómo ver la política de exclusión en los servicios de IA

Puede ver la política de exclusión en vigor de una cuenta desde la páginaAWS Management Console,AWSAPI, oAWS Command Line Interface.

Permisos mínimos

Para ver la política de exclusión en vigor de servicios de IA para una cuenta, debe tener permiso para ejecutar las siguientes acciones:

- `organizations:DescribeEffectivePolicy`
- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations

AWS Management Console

Para ver la política en vigor de una cuenta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la página Cuentas de AWS , elija el nombre de la cuenta para la que desea ver la política de exclusión en vigor de los servicios de IA. Es posible que tenga que expandir las unidades organizativas (elija la opción ▶) para encontrar la cuenta que desea.
3. En la páginaPolíticas, en la pestañaPolíticas de exclusión de servicios de IAElija en la secciónVer la política de IA efectiva para este Cuenta de AWS .

   La consola muestra la directiva efectiva aplicada a la cuenta especificada.

   > **Note**
   >
   > No puede copiar y pegar una política en vigor y usarla como JSON para otra política de exclusión de servicios de IA sin cambios significativos. Los documentos de política de inhabilitación de servicios de IA deben incluirOperadores de herencia (p. 98)que especifican cómo se fusiona cada configuración en la política en vigor final.

AWS CLI & AWS SDKs

Para ver la política en vigor de una cuenta

Puede utilizar uno de los comandos siguientes para ver la política de exclusión en vigor de los servicios de IA:

- AWS CLI:describe-effective-policy

  En el siguiente ejemplo se muestra la política de exclusión efectiva de servicios de IA para una cuenta.

```
$ aws organizations describe-effective-policy \
    --policy-type AISERVICES_OPT_OUT_POLICY \
    --target-id 123456789012
{
    "EffectivePolicy": {
        "PolicyContent": "{\"services\":{\"comprehend\":{\"opt_out_policy\":\"optOut
\"},   ....TRUNCATED FOR BREVITY....   "opt_out_policy\":\"optIn\"}}}",
        "LastUpdatedTimestamp": "2020-12-09T12:58:53.548000-08:00",
        "TargetId": "123456789012",
        "PolicyType": "AISERVICES_OPT_OUT_POLICY"
    }
}
```

- AWSSDK de: DescribeEffectivePolicy

Sintaxis y ejemplos de políticas de exclusión de servicios de IA

En este tema se describe la sintaxis de política de exclusión de servicios de Inteligencia Artificial (AI) y se proporcionan ejemplos.

Sintaxis para políticas de exclusión de servicios de IA

Una política de exclusión de servicios de IA es un archivo de texto sin formato estructurado de acuerdo con las reglas deJSON. La sintaxis de las políticas de exclusión de servicios de IA sigue la sintaxis de los tipos de políticas de administración. Para obtener una discusión completa de esa sintaxis, consulteSintaxis y herencia de políticas para tipos de políticas de administración (p. 97). Este tema se centra en aplicar esa sintaxis general a los requisitos específicos del tipo de política de exclusión de servicios de IA.

> **Important**
>
> La capitalización de los valores que se detallan en esta sección son importantes. Introduzca los valores con letras mayúsculas y minúsculas como se muestra en este tema. Las directivas no funcionan si utiliza mayúsculas inesperadas.

La siguiente directiva muestra la sintaxis básica de política de exclusión de servicios de IA. Si este ejemplo se asociara directamente a una cuenta, dicha cuenta se excluiría explícitamente de un servicio y se optaría por otra. Otras políticas heredadas de niveles superiores (OU o directivas raíz) podrían optar por optar por otros servicios.

```
{
    "services": {
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "lex": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

Imagine la siguiente política de ejemplo asociada a la raíz de la organización. Establece el valor predeterminado para que la organización opte por no participar en todos los servicios de IA. Esto incluye automáticamente cualquier servicio de IA que no esté explícitamente exento de otra manera, incluidos los servicios de IA queAWSPuede desplegarse en el futuro. Puede adjuntar políticas secundarias a unidades organizativas o directamente a cuentas para anular esta configuración para cualquier servicio de IA excepto Amazon Comprehend. La segunda entrada del ejemplo siguiente utiliza`@@operators_allowed_for_child_policies`establecido en`none`Para evitar que se anule. La tercera entrada del ejemplo crea una exención de toda la organización para Amazon Rekognition. Opta en toda la organización por ese servicio, pero la directiva permite que las directivas secundarias se anulen cuando corresponda.

```
{
    "services": {
        "default": {
            "opt_out_policy": {
                "@@assign": "optOut"
```

```
            }
        },
        "comprehend": {
            "opt_out_policy": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

La sintaxis de política de exclusión de servicios de IA incluye los siguientes elementos:

- La`services`Elemento. Una política de exclusión de servicios de IA se identifica con este nombre fijo como el elemento que contiene JSON más externo.

  Una política de exclusión de servicios de IA puede tener una o más sentencias bajo la`services`Elemento. Cada declaración contiene los componentes siguientes:

  - Aclave de nombre de servicioidentifica unAWSServicio de IA. Los siguientes nombres de clave son valores válidos para este campo:
    - **`default`**— representaTodoactualmente disponibles servicios de IA e incluye implícita y automáticamente cualquier servicio de IA que se pueda agregar en el futuro.
    - `codeguruprofiler`
    - `comprehend`
    - `lex`
    - `polly`
    - `rekognition`
    - `textract`
    - `transcribe`
    - `translate`

    Cada declaración de política identificada por una clave de nombre de servicio puede contener los siguientes elementos:

    - La clave de `opt_out_policy`. Esta clave debe estar presente. Esta es la única clave que puede colocar bajo una clave de nombre de servicio.

      La`opt_out_policy`puede contenerSoloel`@@assign`Operador con uno de los siguientes valores:

      - `optOut`: opta por no utilizar contenido para el servicio de IA especificado.
      - `optIn`: elige optar por el uso de contenido para el servicio de IA especificado.

        Notes

        - No puede usar la`@@append`y`@@remove`operadores de herencia en las políticas de exclusión de servicios de IA.
        - No puede usar la`@@enforced_for`en las políticas de exclusión de servicios de IA.
  - En cualquier nivel, puede especificar la propiedad`@@operators_allowed_for_child_policies`para controlar lo que las directivas secundarias pueden hacer para anular la configuración impuesta por las directivas principales. Puede especificar uno de los siguientes valores:
    - `@@assign`— las directivas secundarias de esta política pueden utilizar el`@@assign`para anular el valor heredado con un valor diferente.

- `@@none`: las directivas secundarias de esta política no pueden cambiar el valor.

El comportamiento de la`@@operators_allowed_for_child_policies`depende de dónde lo coloques. Puede utilizar las siguientes ubicaciones:

- En el`services`: controla si una directiva secundaria puede agregar o cambiar la lista de servicios de la directiva efectiva.
- En la clave para un servicio de IA específico o en el`default`clave: controla si una directiva secundaria puede agregar o cambiar la lista de claves bajo esta entrada específica.
- En el`opt_out_policies`para un servicio específico: controla si una directiva secundaria puede cambiar sólo la configuración de este servicio específico.

Ejemplos de políticas de exclusión de servicios de IA

Las políticas de copia de seguridad siguientes son solo para fines informativos.

Ejemplo 1: Inhabilitar todos los servicios de IA para todas las cuentas de la organización

En el siguiente ejemplo se muestra una directiva que puede adjuntar a la raíz de su organización para deshabilitar los servicios de IA para las cuentas de su organización.

Tip

Si copia el siguiente ejemplo utilizando el botón Copiar en la esquina superior derecha del ejemplo, la copia no incluye los números de línea. Está listo para pegar.

```
    | {
    |     "services": {
[1] |         "@@operators_allowed_for_child_policies": ["@@none"],
    |         "default": {
[2] |             "@@operators_allowed_for_child_policies": ["@@none"],
    |             "opt_out_policy": {
[3] |                 "@@operators_allowed_for_child_policies": ["@@none"],
    |                 "@@assign": "optOut"
    |             }
    |         }
    |     }
    | }
```

- [1] — El`"@@operators_allowed_for_child_policies": ["@@none"]`que está en`services`impide que cualquier directiva secundaria agregue secciones nuevas para servicios individuales que no sean`default`que ya está allí.`Default`es el marcador de posición que representa «todos los servicios de IA».
- [2] — El`"@@operators_allowed_for_child_policies": ["@@none"]`que está en`default`impide que las directivas secundarias agreguen secciones nuevas que no sean las`opt_out_policy`que ya está allí.
- [3] — El`"@@operators_allowed_for_child_policies": ["@@none"]`que está en`opt_out_policy`Evita que las políticas secundarias cambien el valor de`optOut`o agregando cualquier configuración adicional.

Ejemplo 2: Establecer una configuración predeterminada de la organización para todos los servicios, pero permitir que las directivas secundarias anulen la configuración de los servicios individuales

En el siguiente ejemplo de directiva se establece un valor predeterminado para toda la organización para todos los servicios de IA. El valor para`default`impide que una directiva secundaria cambie el`optOut`valor para el servicio`default`, el marcador de posición para todos los servicios de IA. Si esta directiva se aplica como directiva principal adjuntándola a la raíz o a una unidad organizativa, las directivas secundarias pueden cambiar la configuración de exclusión de servicios individuales, como se muestra en la segunda directiva.

- Porque no hay`"@@operators_allowed_for_child_policies": ["@@none"]`En el`services`, las directivas secundarias pueden agregar nuevas secciones para servicios individuales.
- La`"@@operators_allowed_for_child_policies": ["@@none"]`que está en`default`impide que las directivas secundarias agreguen secciones nuevas que no sean las`opt_out_policy`que ya está allí.
- La`"@@operators_allowed_for_child_policies": ["@@none"]`que está en`opt_out_policy`Evita que las políticas secundarias cambien el valor de`optOut`o agregando cualquier configuración adicional.

Política principal de exclusión de servicios de IA raíz de la organización

```
{
    "services": {
        "default": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "opt_out_policy": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
        }
    }
}
```

En la siguiente directiva de ejemplo se supone que la directiva de ejemplo anterior está asociada a la raíz de la organización o a una unidad organizativa principal y que se adjunta este ejemplo a una cuenta afectada por la directiva principal. Anula la configuración predeterminada de exclusión y opta explícitamente solo por el servicio Amazon Lex.

Política de exclusión infantil de servicios de IA

```
{
    "services": {
        "lex": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

La política efectiva resultante para el Cuenta de AWS es que la cuenta solo acepta Amazon Lex y opta por no participar en todas las demásAWSservicios de IA debido a la heredada`default`opción de exclusión de la directiva principal.

Ejemplo 3: Definir una política de exclusión de servicios de IA de toda la organización para un único servicio

En el siguiente ejemplo se muestra una política de exclusión de servicios de IA que define un`optOut`para un único servicio de IA. Si esta directiva está adjunta a la raíz de la organización, impide que cualquier directiva secundaria anule la`optOut`para este servicio. Otros servicios no se abordan en esta política, pero podrían verse afectados por las políticas secundarias de otras unidades organizativas o cuentas.

```
{
    "services": {
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optOut",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        }
    }
}
```

Políticas de copia de seguridad

Para obtener información y procedimientos comunes a todos los tipos de políticas, consulte los siguientes temas:

- Habilitar y desactivar tipos de políticas (p. 87)
- Obtenga detalles sobre las políticas (p. 90)
- Sintaxis y herencia de políticas (p. 95)

AWS Backuple permite crearPlanes de copiaDeterminación de cómo realizar una copia de seguridad de suAWSde AWS. Las reglas del plan incluyen una variedad de configuraciones, como la frecuencia de las copias de seguridad, la ventana de tiempo durante la cual se realiza la copia de seguridad, el Región de AWS Contiene los recursos de que va a realizar una copia de seguridad y el almacén en el que se almacenará la copia de seguridad. A continuación, puede aplicar un plan de copia de seguridad a grupos de recursos de AWS identificados mediante etiquetas. También debe identificar unAWS Identity and Access Management(IAM) que otorgaAWS BackupPara realizar la operación de copia de seguridad en su nombre.

Las políticas de copia de seguridad de AWS Organizations combinan todos esos elementos en documentos de texto JSON . Puede asociar una política de copia de seguridad a cualquiera de los elementos de la estructura de su organización, como la raíz, las unidades organizativas (OU) y las cuentas individuales. Las Organizations aplican reglas de herencia para combinar las políticas de la raíz de la organización, de las unidades organizativas principales o asociadas a la cuenta. Esto da como resultado una política de copia de seguridad en vigor (p. 175) para cada cuenta. Esta política en vigor indica a AWS Backup cómo realizar copias de seguridad de los recursos de AWS automáticamente.

Las políticas de copia de seguridad le proporcionan un control detallado sobre las copias de seguridad de sus recursos en cualquier nivel que requiera su organización. Por ejemplo, puede especificar en una política asociada a la raíz de la organización que se debe realizar una copia de seguridad de todas las tablas de Amazon DynamoDB. Esa política puede incluir una frecuencia de copia de seguridad predeterminada. A continuación, puede asociar una política de copia de seguridad a las unidades organizativas que sobrescriben la frecuencia de la copia de seguridad de acuerdo con los requisitos de cada unidad organizativa. Por ejemplo, la unidad organizativa `Developers` puede especificar una frecuencia de copia de seguridad de una vez por semana, mientras que la unidad organizativa `Production` especifica una vez por día.

Puede crear políticas de copia de seguridad parciales que solo incluyan una parte de la información necesaria para realizar correctamente la copia de seguridad de sus recursos. Puede asociar estas políticas a diferentes partes del árbol de la organización, como la raíz o una unidad organizativa principal, con la intención de que las unidades organizativas y cuentas de nivel inferior hereden esas políticas parciales. Cuando las Organizations combinan todas las políticas de una cuenta mediante reglas de herencia, la política en vigor resultante debe tener todos los elementos necesarios. De lo contrario,AWS Backupconsidera que la política no es válida y no hace una copia de seguridad de los recursos afectados.

> **Important**
>
> AWS Backup solo puede realizar una copia de seguridad correcta si le invoca una política en vigor completa que tiene todos los elementos necesarios.
> Aunque una estrategia de política parcial como la descrita anteriormente puede funcionar, si una política en vigor para una cuenta está incompleta, se producirán errores o se producirán recursos de los que no se realicen correctamente las copias de seguridad. Como estrategia alternativa, plantéese exigir que todas las políticas de copia de seguridad estén completas y sean válidas por sí mismas. Utilice los valores predeterminados proporcionados por las políticas asociadas a un nivel más alto en la jerarquía y reemplácelos cuando sea necesario en las políticas secundarias mediante la inclusión de operadores de control secundarios de herencia (p. 98).

El plan de copia de seguridad eficaz para cada Cuenta de AWS aparece en la organización en elAWS Backupcomo un plan inmutable para esa cuenta. Puede verlo, pero no cambiarlo.

Cuando AWS Backup inicia una copia de seguridad basada en un plan de copia de seguridad creado por la política, puede ver el estado del trabajo de copia de seguridad en la consola de AWS Backup. Un usuario de una cuenta miembro puede ver el estado y los errores de los trabajos de copia de seguridad de esa cuenta miembro. Si también habilita el acceso al servicio de confianza conAWS Backup, un usuario de la cuenta de administración de la organización puede ver el estado y los errores de todos los trabajos de copia de seguridad de la organización. Para obtener más información, consulteCómo habilitar la administración entre cuentasen laAWS BackupGuía para desarrolladores.

Introducción a las políticas de copia de seguridad

Siga estos pasos para empezar a utilizar las políticas de copia de seguridad.

1. Obtenga información acerca de los permisos que debe tener para realizar tareas de políticas de copia de seguridad (p. 162).
2. Obtenga más información sobre algunas prácticas que recomendamos al utilizar políticas de copia de seguridad (p. 163).
3. Habilite políticas de copia de seguridad para su organización (p. 87).
4. Crear una política de copias de seguridad (p. 164).
5. Asocie la política de copia de seguridad a la raíz, unidad organizativa o cuenta de su organización (p. 173).
6. Vea la política de copia de seguridad en vigor combinada que se aplica a una cuenta (p. 175).

Para todos estos pasos, debe iniciar sesión como usuario de IAM, asumir un rol de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.

Información adicional

- Aprenda la sintaxis de las políticas de copia de seguridad y vea ejemplos de políticas (p. 177)

Requisitos previos y permisos para administrar políticas de copia de seguridad

En esta página se describen los requisitos previos y los permisos necesarios para administrar políticas de copia de seguridad enAWS Organizations.

Temas

Requisitos previos para administrar políticas de copia de seguridad

Para administrar políticas de copia de seguridad en una organización, es necesario lo siguiente:

- Su organización debe tener habilitadas todas las características (p. 37).
- Debe haber iniciado sesión en la cuenta de administración de su organización.
- SusAWS Identity and Access ManagementDebe contar con los permisos que se enumeran en la siguiente sección.

Permisos para administrar políticas de copia de seguridad

El siguiente ejemplo de política de IAM proporciona permisos para administrar todos los aspectos de las políticas de copia de seguridad de una organización.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageBackupPolicies",
            "Effect": "Allow",
            "Action": [
                "organizations:AttachPolicy",
                "organizations:CreatePolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeAccount",
                "organizations:DescribeCreateAccountStatus",
                "organizations:DescribeEffectivePolicy",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribePolicy",
                "organizations:DetachPolicy",
                "organizations:DisableAWSServiceAccess",
                "organizations:DisablePolicyType",
                "organizations:EnableAWSServiceAccess",
                "organizations:EnablePolicyType",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListCreateAccountStatus",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPolicies",
                "organizations:ListPoliciesForTarget",
                "organizations:ListRoots",
```

```
                "organizations:ListTargetsForPolicy",
                "organizations:UpdatePolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Para obtener más información acerca de las políticas y los permisos de IAM, consulte laIAM User Guide.

Prácticas recomendadas para el uso de políticas de copia de seguridad

AWS recomienda las siguientes prácticas para el uso de políticas de copia de seguridad:

Decidir una estrategia de política de copia de seguridad

Puede crear políticas de copia de seguridad en partes incompletas que se heredan y fusionan para crear una política completa para cada cuenta de miembro. Si lo hace, corre el riesgo de terminar con una política en vigor incompleta si realiza un cambio en un nivel sin considerar detenidamente el impacto del cambio en todas las cuentas que estén por debajo de ese nivel. Para que esto no ocurra, le recomendamos que se asegure de que las políticas de copia de seguridad que implemente en todos los niveles estén completas por sí mismas. Trate las políticas principales como políticas predeterminadas que se pueden reemplazar por la configuración especificada en las políticas secundarias. De esta forma, incluso aunque no exista una política secundaria, la política heredada estará completa y utilizará los valores predeterminados. Puede controlar qué configuración se puede añadir, cambiar o eliminar en las políticas secundarias mediante los operadores de herencia de control secundarios (p. 99).

Valide los cambios realizados en sus políticas de copia de seguridad mediante `GetEffectivePolicy`

Cuando realice un cambio en una política de copia de seguridad, compruebe las políticas en vigor de cuentas representativas que estén por debajo del nivel en el que haya realizado el cambio. Puede ver la política en vigor mediante la AWS Management Console (p. 175) o mediante la operación de la API GetEffectivePolicy o una de sus variantes de SDK de la AWS CLI o AWS. Asegúrese de que el cambio que ha realizado haya tenido el impacto previsto en la política en vigor.

Comience de forma sencilla y haga pequeños cambios

Para simplificar la depuración, comience con políticas sencillas y realice cambios de un elemento cada vez. Valide el comportamiento y el impacto de cada cambio antes de realizar el siguiente cambio. Este enfoque reduce el número de variables que tiene que tener en cuenta cuando se produce un error o un resultado inesperado.

Almacene copias de sus copias de seguridad en otros Regiones de AWS Cuentas de la organización

Para mejorar su posición de recuperación ante desastres, puede almacenar copias de sus copias de seguridad.

- Una región diferente— Si almacena copias de la copia de seguridad en Regiones de AWS , ayuda a proteger la copia de seguridad contra daños accidentales o eliminaciones en la región original. Usar`copy_actions`de la directiva para especificar un almacén en una o varias regiones de la misma

cuenta en la que se ejecuta el plan de copia de seguridad. Para ello, identifique la cuenta mediante el`$account`Cuando especifique el ARN del almacén de copia de seguridad en el que se almacenará la copia de seguridad de. La`$account` se reemplaza automáticamente en tiempo de ejecución con el ID de cuenta en el que se está ejecutando la directiva de copia de seguridad.

- Una cuenta diferente— Si almacena copias de la copia de seguridad en Cuentas de AWS , añade una barrera de seguridad que ayuda a proteger contra un actor malintencionado que pone en peligro una de sus cuentas. Usar`copy_actions`de la directiva para especificar un almacén en una o varias cuentas de la organización, independientemente de la cuenta en la que se ejecuta el plan de copia de seguridad. Para ello, identifique la cuenta utilizando su número de ID de cuenta real cuando especifique el ARN del almacén de copia de seguridad en el que almacenar la copia de la copia de seguridad.

Limite el número de planes por política

En las políticas que contienen varios planes es más complicado solucionar problemas ya que hay que validar un mayor número de salidas. Por ello, le recomendamos que haga que cada política contenga un solo plan de copia de seguridad para simplificar la depuración y la resolución de problemas. A continuación, puede añadir más políticas con otros planes para cumplir con otros requisitos. Este enfoque ayuda a mantener los problemas de un plan aislados en una política y evita que esos problemas compliquen la resolución de problemas con otras políticas y sus planes.

Utilice conjuntos de pilas para crear los almacenes de copias de seguridad y los roles de IAM necesarios

UsarAWS CloudFormationLa integración de conjuntos de pilas con Organizations para crear automáticamente los almacenes de copias de seguridad necesarios yAWS Identity and Access Management(IAM) en cada una de las cuentas miembro de su organización. Puede crear un conjunto de pilas que incluya los recursos que desea que estén disponibles automáticamente en cada Cuenta de AWS En su organización. Este enfoque le permite ejecutar sus planes de copia de seguridad con la seguridad de que las dependencias ya se cumplen. Para obtener más información, consulteCreación de un conjunto de pilas con permisos autoadministradosen laAWS CloudFormationGuía del usuario de.

Compruebe sus resultados revisando la primera copia de seguridad creada en cada cuenta

Cuando realice un cambio en una política, compruebe la siguiente copia de seguridad creada después de ese cambio para asegurarse de que el cambio tuvo el impacto deseado. Este paso va más allá de examinar la política en vigor y garantiza queAWS Backupinterprete sus políticas e implemente los planes de copia de seguridad de la manera que pretendía.

Crear, actualizar y eliminar políticas de copia de seguridad

En este tema:

- Después de tihabilitar políticas de copia de seguridad (p. 87)para su organización, puedeCrear una política (p. 165).
- Cuando cambien sus requisitos de copia de seguridad, puede actualizar una política existente (p. 168).
- Cuando ya no necesite una política y después de desasociarla de todas las unidades organizativas (OU) y cuentas, puedeborrarlo (p. 171).

Creación de un plan de copia de seguridad

Permisos mínimos

Para crear una política de copia de seguridad, necesita permiso para ejecutar la siguiente acción:

- `organizations:CreatePolicy`

AWS Management Console

Puede crear una política de copia de seguridad en la AWS Management Console de una de estas dos maneras:

- Un editor visual que le permite elegir opciones y generar el texto de la política JSON automáticamente.
- Un editor de texto que le permite crear directamente el texto de la política JSON usted mismo.

El editor visual facilita el proceso, pero limita su flexibilidad. Es una excelente manera de crear sus primeras políticas y sentirse cómodo al usarlas. Cuando comprenda cómo funcionan y haya comenzado a verse limitado por lo que ofrece el editor visual, puede añadir características avanzadas a sus políticas editando el texto de la política JSON usted mismo. El editor visual utiliza sólo elOperador de configuración de valores @ @assign (p. 99), y no proporciona ningún acceso a laOperadores de control secundarios (p. 99). Solo puede agregar los operadores de control secundario si edita manualmente el texto de la política JSON.

Para crear una política de backup

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la página Backup policies (Políticas de copia de seguridad), seleccione Create policy (Crear política).
3. En la páginaCrear política, ingrese unaNombre de la políticay unDescripción de la política.
4. (Opcional) Puede agregar una o varias etiquetas a la política seleccionandoAñada etiquetaA continuación, introduzca una clave y un valor opcional. Dejar el valor en blanco lo establece en una cadena vacía; no es`null`. Puede adjuntar hasta 50 etiquetas a una política. Para obtener más información acerca del etiquetado, consulte Etiquetado de recursos de AWS Organizations (p. 229).
5. Puede crear la política mediante el Visual editor (Editor visual) como se describe en este procedimiento. También puede especificar o pegar texto de política en la listaJSONPestaña. Para obtener información sobre la sintaxis de políticas de copia de seguridad, consulteEjemplos y sintaxis de políticas de copia de seguridad (p. 177).

   Si decide utilizar el Visual editor (Editor visual), seleccione las opciones de copia de seguridad adecuadas para su situación. Un plan de copia de seguridad consta de tres partes. Para obtener más información sobre estos elementos del plan de copia de seguridad, consulte.Crear un plan de copia de seguridadyAsignación de recursosen laAWS BackupGuía para desarrolladores.

   a. Detalles generales del plan de Backup de
      - LaEl nombre del plan de BackupPuede constar únicamente de caracteres alfanuméricos, guiones y guiones bajos.
      - Debe seleccionar al menos una región del plan de copia de seguridad de la lista. El plan solo puede realizar copias de seguridad de recursos en los archivos seleccionados Regiones de AWS .

b. Una o más reglas de copia de seguridad que especifican cómo y cuándo debe funcionar AWS Backup. Cada regla de copia de seguridad define los siguientes elementos:

- Una programación que incluye la frecuencia de la copia de seguridad y la ventana de tiempo en la que se puede realizar la copia de seguridad.
- El nombre del almacén de copia de seguridad que se va a utilizar. El nombre del almacén de copia de seguridad puede constar únicamente de caracteres alfanuméricos, guiones y guiones bajos. Debe haber un almacén de copia de seguridad para que el plan pueda ejecutarse correctamente. Cree el almacén mediante la consola de AWS Backup o los comandos de AWS CLI.
- (Opcional) Uno o variosCopiar en regiónTambién copie la copia de seguridad en almacenes de otros Regiones de AWS .
- Uno o más pares de clave y valor de etiqueta para asociar a los puntos de recuperación de copia de seguridad creados cada vez que se ejecuta este plan de copia de seguridad.
- Opciones de ciclo de vida que especifican cuándo pasa la copia de seguridad al almacenamiento en frío y cuándo caduca la copia de seguridad.

SeleccionarAñada reglapara agregar cada regla que necesite al plan.

Para obtener más información sobre las reglas de copia de seguridad, consulteReglas de copia de seguridaden laAWS BackupGuía para desarrolladores.

c. Una asignación de recursos que especifica qué recursosAWS BackupDebe realizar una copia de seguridad con este plan. La asignación se realiza especificando pares de etiquetas queAWS Backuputiliza para buscar y hacer coincidir recursos

- El nombre de la asignación de recursos puede constar únicamente de caracteres alfanuméricos, guiones y guiones bajos.
- Especifique la propiedadRol de IAM: paraAWS BackupPara realizar la copia de seguridad por su nombre.

  En la consola, no especifique todo el nombre de recurso de Amazon (ARN). Debe incluir tanto el nombre del rol como su prefijo, que especifica el tipo de rol. Los prefijos son típicamente`role`or`service-role`Y están separados del nombre del rol por una barra inclinada ('/'). Por ejemplo, puede escribir `role/MyRoleName` o `service-role/MyManagedRoleName`. Esto se convierte en un ARN completo para usted cuando se almacena en el JSON subyacente.

  > **Important**
  >
  > La función de IAM especificada ya debe existir en la cuenta a la que se aplica la política. De lo contrario, el plan de copia de seguridad podrá iniciar correctamente trabajos de copia de seguridad, pero dichos trabajos de copia de seguridad fallarán.

- Especifique una o másClave de etiqueta de recursosyValores de etiquetaPara identificar los recursos de los que desea realizar copias de seguridad. Si hay más de un valor de etiqueta, sepárelos con comas.

SeleccionarAgregar asignaciónPara agregar cada asignación de recursos configurada al plan de copia de seguridad.

Para obtener más información, consulteAsigne recursos a un plan de copias de seguridaden laAWS BackupGuía para desarrolladores.

6. Cuando haya terminado de crear la política, seleccioneCrear política. La política aparece en la lista de políticas de copia de seguridad disponibles.

AWS CLI & AWS SDKs

Para crear una política de backup

Puede utilizar uno de los siguientes elementos para crear una política de copia de seguridad:

- AWS CLI: create-policy

  Cree un plan de copia de seguridad como texto JSON similar al siguiente y guárdela en un archivo de texto. Para obtener reglas completas para la sintaxis, consulteEjemplos y sintaxis de políticas de copia de seguridad (p. 177).

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { "@@assign": [ "ap-northeast-2", "us-east-1", "eu-
north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 5/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "complete_backup_window_minutes": { "@@assign": "10080" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "180" },
                        "delete_after_days": { "@@assign": "270" }
                    },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:secondary-
vault": {
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "10" },
                                "delete_after_days": { "@@assign": "100" }
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                        "tag_key": { "@@assign": "dataType" },
                        "tag_value": { "@@assign": [ "PII" ] }
                    }
                }
            }
        }
    }
}
```

Este plan de copia de seguridad especifica queAWSLa copia de seguridad debe realizar una copia de seguridad de todos los recursos del Cuentas de AWS que se encuentran en el Regiones de AWS y que tienen la etiquetadataTypecon un valor dePII.

A continuación, importe el plan de copia de seguridad del archivo de política JSON para crear una nueva política de copia de seguridad en la organización. Anote el ID de política que viene al final del ARN de política en el resultado.

```
$ aws organizations create-policy \
    --name "MyBackupPolicy" \
    --type BACKUP_POLICY \
    --description "My backup policy" \
    --content file://policy.json{
```

```
    "Policy": {
        "PolicySummary": {
            "Arn": "arn:aws:organizations::o-aa111bb222:policy/backup_policy/p-
i9j8k7l6m5",
            "Description": "My backup policy",
            "Name": "MyBackupPolicy",
            "Type": "BACKUP_POLICY"
        }
        "Content": "...a condensed version of the JSON policy document you provided
 in the file...",
    }
}
```

- AWSSDK: CreatePolicy

Qué hacer a continuación

Cuando haya creado una política de copia de seguridad, puede hacerla efectiva. Para hacer eso, puedesAsociar la política (p. 209)A la raíz de la organización, las unidades organizativas (OU), Cuentas de AWS dentro de su organización, o una combinación de todos ellos.

Actualización de una política de copia de seguridad

Cuando inicia sesión en la cuenta de administración de su organización, puede editar una política que requiera cambios en la organización.

Permisos mínimos

Para actualizar una política de copia de seguridad, debe tener permiso para ejecutar las siguientes acciones:

- `organizations:UpdatePolicy` con un elemento `Resource` en la misma instrucción de política que incluye el ARN de la política que actualizar (o "*")
- `organizations:DescribePolicy` con un elemento `Resource` en la misma instrucción de política que incluye el ARN de la política que actualizar (o "*")

AWS Management Console

Para actualizar una política de copia de seguridad

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaPolíticas de copia de seguridadElija el nombre de la política que desea actualizar.
3. Elija Edit policy (Editar política).
4. Puede introducir un nuevoNombre de la política,Descripción de la política. Puede cambiar el contenido de la política mediante la herramientaVisual editor (Editor visual)o editando directamente elJSON.
5. Cuando haya terminado de actualizar la política, elija Save changes (Guardar cambios).

AWS CLI & AWS SDKs

Para actualizar una política de copia de seguridad

Puede utilizar uno de los siguientes elementos para actualizar una política de copia de seguridad:

- AWS CLI:update-policy

El siguiente ejemplo cambia el nombre de una política de copia de seguridad.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}"
    }
}
```

En el siguiente ejemplo se agrega o cambia la descripción de una política de copia de seguridad.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
       "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}"
    }
}
```

En el ejemplo siguiente se cambia el documento de directiva JSON adjunto a una directiva de copia de seguridad. En este ejemplo, el contenido se toma de un archivo llamado`policy.json`por el texto siguiente:

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { "@@assign": [ "ap-northeast-2", "us-east-1", "eu-
north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 5/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "complete_backup_window_minutes": { "@@assign": "10080" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "180" },
                        "delete_after_days": { "@@assign": "270" }
                    },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "copy_actions": {
```

```
                        "arn:aws:backup:us-east-1:$account:backup-vault:secondary-
vault": {
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "10" },
                                "delete_after_days": { "@@assign": "100" }
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                        "tag_key": { "@@assign": "dataType" },
                        "tag_value": { "@@assign": [ "PII" ] }
                    }
                }
            }
        }
    }
}
```

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}}"
}
```

- AWSSDK: UpdatePolicy

Edición de etiquetas adjuntas a una directiva de copia de seguridad

Cuando inicia sesión en la cuenta de administración de su organización, puede agregar o eliminar las etiquetas adjuntas a una política de copia de seguridad. Para obtener más información acerca del etiquetado, consulte Etiquetado de recursos de AWS Organizations (p. 229).

Permisos mínimos

Para editar las etiquetas adjuntas a una política de copia de seguridad en suAWSDebe tener los siguientes permisos:

- `organizations:DescribeOrganization`(sólo consola — para navegar a la directiva)
- `organizations:DescribePolicy`(sólo consola — para navegar a la directiva)
- `organizations:TagResource`

- `organizations:UntagResource`

AWS Management Console

Para editar las etiquetas adjuntas a una directiva de copia de seguridad

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. Políticas de copia de seguridadpage
3. Elija el nombre de la política con las etiquetas que desea editar.

   Aparece la página de detalles de política.
4. En la pestaña Tags (Etiquetas), elija Manage tags (Administrar etiquetas).
5. Puede realizar cualquiera de estas acciones en esta página:
   - Edite el valor de cualquier etiqueta introduciendo un nuevo valor sobre el anterior. No se puede modificar la clave. Para cambiar una clave, debe eliminar la etiqueta con la clave anterior y agregar una etiqueta con la nueva clave.
   - Elimine una etiqueta existente seleccionandoRemove.
   - Agregue una clave de etiqueta y un par de valor. SeleccionarAñada etiquetay, a continuación, introduzca el nuevo nombre de clave y el valor opcional en los cuadros proporcionados. Si deja elValorEn blanco, el valor es una cadena vacía;`null`.
6. SeleccionarGuarde los cambiosdespués de haber realizado todas las adiciones, eliminaciones y ediciones que desee realizar.

AWS CLI & AWS SDKs

Para editar las etiquetas adjuntas a una directiva de copia de seguridad

Puede utilizar uno de los siguientes comandos para editar las etiquetas asociadas a una política de copia de seguridad:

- AWS CLI:tag-resourceyuntag-resource
- AWSSDK: TagResourceyUntagResource

Eliminar una política de copia de seguridad

Cuando inicia sesión en la cuenta de administración de su organización, puede eliminar una política que ya no necesite en su organización.

Para poder eliminar una política, primero debe desasociarla de todas las entidades asociadas.

Permisos mínimos

Para eliminar una política, debe tener permiso para ejecutar la siguiente acción:

- `organizations:DeletePolicy` con un elemento `Resource` en la misma instrucción de política que incluye el ARN de la política que eliminar (o "*")

AWS Management Console

Para eliminar una política de copia de seguridad

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaPolíticas de copia de seguridadElija el nombre de la política de copia de seguridad que desea ver.
3. En primer lugar, debe desasociar la política de copia de seguridad que desea eliminar de todas las raíces, unidades organizativas y cuentas. Elija el iconoimplementaciónElija el botón de opción situado junto a cada raíz, unidad organizativa o cuenta que se muestra en la pestañaimplementacióny, a continuación, elijaSeparar. En el cuadro de diálogo de confirmación, elijaSeparar. Repita la operación hasta que elimine todos los destinos.
4. SeleccionarEliminarEn la parte superior de la página.
5. En el cuadro de diálogo de confirmación, escriba el nombre de la política y, a continuación, elijaEliminar.

AWS CLI & AWS SDKs

Para eliminar una política de copia de seguridad

Puede utilizar uno de los comandos siguientes para eliminar una política:

- AWS CLI: delete-policy

  En el ejemplo siguiente se elimina la política especificada. Solo funciona si la política no está asociada a ninguna raíz, unidad organizativa o cuenta.

```
$ aws organizations delete-policy \
    --policy-id p-i9j8k7l6m5
```

  Este comando no genera ninguna salida cuando se realiza correctamente.
- AWSSDK: DeletePolicy

Asociar y desasociar políticas de copia de seguridad

Puede utilizar las políticas de copia de seguridad en toda una organización además de en las unidades organizativas (OU) y las cuentas individuales. Tenga en cuenta los siguientes puntos:

- Cuando asocia una política de copia de seguridad a la raíz de su organización, la política de copia de seguridad se aplica a todas las cuentas y unidades organizativas de los miembros de la raíz.
- Cuando asocia una política de copia de seguridad a una unidad organizativa, esa política se aplica a las cuentas que pertenecen a la unidad organizativa o a cualquiera de sus unidades organizativas secundarias. Esas cuentas también están sujetas a cualquier política de copia de seguridad asociada a la raíz de la organización.
- Cuando se adjunta una política de copia de seguridad a unaccount, esa política sólo se aplica a esa cuenta. La cuenta también está sujeta a cualquier política asociada a la raíz de la organización y a las unidades organizativas a las que pertenezca la cuenta.

La agregación de cualquier política de copia de seguridad que hereda la cuenta de las unidades organizativas raíz y principales, así como de cualquier política directamente asociada a la cuenta, es laPolítica en vigor (p. 175). Para obtener información sobre cómo se fusionan las políticas con la política en vigor, consulte Sintaxis y herencia de políticas para tipos de políticas de administración (p. 97).

Asociar una política de copia de seguridad

Cuando inicia sesión en la cuenta de administración de su organización, puede asociar una política de copia de seguridad a la raíz de la organización, unidad organizativa o directamente a una cuenta.

Permisos mínimos

Para asociar políticas de copia de seguridad, debe tener permiso para ejecutar la siguiente acción:

- `organizations:AttachPolicy`

AWS Management Console

Puede asociar una política de copia de seguridad navegando hasta la política o hasta la raíz, unidad organizativa o cuenta a la que desee adjuntar la política.

Para asociar una política de copia de seguridad navegando a la raíz, unidad organizativa o cuenta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la página Cuentas de AWS , seleccione el nombre de la raíz, unidad organizativa o cuenta a la que desea adjuntar una política. Es posible que tenga que expandir las unidades organizativas (elija la opción ▶) para encontrar la unidad organizativa o la cuenta que desea.
3. En el navegadorPolíticas, en la entrada dePolíticas de copia de seguridad, elijaAttach.
4. Busque la política que desea y elijaAsociar política.

   La lista de políticas de copia de seguridad asociadas en elPolíticasse actualiza para incluir la nueva adición. El cambio de política surtirá efecto de inmediato.

Para adjuntar una directiva de copia de seguridad navegando a la directiva

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaPolíticas de copia de seguridadElija el nombre de la política que desea asociar.
3. En la páginaimplementación, elijaAttach.
4. Elija el botón de opción situado junto a la raíz, unidad organizativa o cuenta a la que desea adjuntar la política. Es posible que tenga que expandir las unidades organizativas (elija la opción ▶) para encontrar la unidad organizativa o la cuenta que desea.
5. Elija Attach policy.

   La lista de políticas de copia de seguridad asociadas en elimplementaciónse actualiza para incluir la nueva adición. El cambio de política surtirá efecto de inmediato.

AWS CLI & AWS SDKs

Para asociar una política de copia de seguridad a la raíz de la organización, la OU o la cuenta

Puede utilizar uno de los siguientes comandos para adjuntar una política de copia de seguridad:

- AWS CLI:attach-policy

```
$ aws organizations attach-policy \
```

```
    --target-id 123456789012 \
    --policy-id p-i9j8k7l6m5
```

- AWSSDK: AttachPolicy

El cambio de política surtirá efecto de inmediato.

Desasociar una política de copia de seguridad

Cuando inicia sesión en la cuenta de administración de su organización, puede desasociar una política de copia de seguridad de la raíz de la organización, unidad organizativa o cuenta a la que está asociada. Después de desasociar una política de copia de seguridad de una entidad, dicha política ya no se aplica a ninguna cuenta que estuviera afectada por la entidad ahora desasociada. Para desasociar una política, siga los pasos que se describen a continuación.

Permisos mínimos

Para desasociar una política de copia de seguridad de la raíz de una organización, unidad organizativa o cuenta, debe tener permiso para ejecutar la siguiente acción:

- `organizations:DetachPolicy`

AWS Management Console

Puede desasociar una política de copia de seguridad navegando hasta la política o hasta la raíz, unidad organizativa o cuenta de la que desea desasociar la política.

Para desasociar una política de copia de seguridad, vaya a la raíz, unidad organizativa o cuenta a la que esté asociada.

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la página Cuentas de AWS Vaya a la raíz, unidad organizativa o cuenta de la que desea desasociar una política. Es posible que tenga que expandir las unidades organizativas (elija la opción▶) para encontrar la unidad organizativa o la cuenta que desea. Elegir el nombre de la raíz, la OU o la cuenta.
3. En la páginaPolíticasEn la pestaña, elija el botón de opción situado junto a la política de copia de seguridad que desea desasociar y, a continuación, elijaSeparar.
4. En el cuadro de diálogo de confirmación, elijaPolítica de desvinculación.

   La lista de políticas de copia de seguridad asociadas se actualiza. El cambio de política surtirá efecto de inmediato.

Para separar una directiva de copia de seguridad navegando hasta la directiva

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaPolíticas de copia de seguridadElija el nombre de la política que desea desasociar de una raíz, unidad organizativa o cuenta.
3. En la páginaimplementación, elija el botón de opción situado junto a la raíz, unidad organizativa o cuenta de la que desea desasociar la política. Es posible que tenga que expandir las unidades organizativas (elija la opción▶) para encontrar la unidad organizativa o la cuenta que desea.
4. Elija Detach (Desasociar).

5. En el cuadro de diálogo de confirmación, elijaSeparar.

   La lista de políticas de copia de seguridad asociadas se actualiza. El cambio de política surtirá efecto de inmediato.

AWS CLI & AWS SDKs

Para desasociar una política de copia de seguridad de la raíz de la organización, la unidad organizativa o la cuenta

Puede utilizar uno de los siguientes comandos para desasociar una política de copia de seguridad:

- AWS CLI:detach-policy

  En el ejemplo siguiente se desconecta una directiva de una unidad organizativa.

```
$ aws organizations detach-policy \
    --target-id ou-a1b2-f6g7h222 \
    --policy-id p-i9j8k7l6m5
```

  Este comando no genera ninguna salida cuando se realiza correctamente.
- AWSSDK: DetachPolicy

El cambio de política surtirá efecto de inmediato.

Ver políticas de copia de seguridad en vigor

Puede ver la política de copia de seguridad en vigor de una cuenta desde la páginaAWSConsola de administraciónAWSAPI, oAWSInterfaz de línea de comandos. En la sección siguiente se proporciona una breve descripción general de la política de copia de seguridad efectiva, incluido un ejemplo.

¿Cuál es la política de copia de seguridad en vigor?

LaPolítica de copia de seguridad efectivaEspecifica la configuración final del plan de copia de seguridad que se aplica a un Cuenta de AWS . Es la agregación de cualquier política de copia de seguridad que hereda la cuenta, además de cualquier política de copia de seguridad asociada directamente a la cuenta. Cuando asocia una política de copia de seguridad a la raíz de la organización, esta se aplica a todas las cuentas de la organización. Cuando asocia una política de copia de seguridad a una unidad organizativa (OU), esta se aplica a todas las cuentas y unidades organizativas que pertenecen a la unidad organizativa (OU). Cuando se asocia una política directamente a una cuenta, solo se aplica a esa cuenta. Cuenta de AWS .

Por ejemplo, la política de copia de seguridad asociada a la raíz de la organización puede especificar que todas las cuentas de la organización hagan una copia de seguridad de todas las tablas de Amazon DynamoDB con una frecuencia de copia de seguridad predeterminada de una vez por semana. Una política de copia de seguridad independiente asociada directamente a una cuenta miembro con información fundamental en una tabla puede anular la frecuencia con un valor de una vez al día. La combinación de estas políticas de copia de seguridad compone la política de copia de seguridad en vigor. Esta política de copia de seguridad en vigor se determina de forma individual para cada cuenta de la organización. En este ejemplo, el resultado es que todas las cuentas de la organización hagan una copia de seguridad de sus tablas de DynamoDB una vez por semana, excepto una cuenta que realiza una copia de seguridad de sus tablas diariamente.

Para obtener información acerca de cómo se combinan las políticas de copia de seguridad en la política de copia de seguridad en vigor final, consulteSintaxis y herencia de políticas para tipos de políticas de administración (p. 97).

Ver la política de copia de seguridad en vigor

Puede ver la política de copia de seguridad en vigor de una cuenta mediante la herramientaAWS Management Console,AWSAPI, oAWS Command Line Interface.

Permisos mínimos

Para ver la política de copia de seguridad en vigor de una cuenta, debe tener permiso para ejecutar las siguientes acciones:

- `organizations:DescribeEffectivePolicy`
- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations

AWS Management Console

Para ver la política en vigor de una cuenta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la página Cuentas de AWS Elija el nombre de la cuenta para la que desea ver la política de copia de seguridad en vigor. Es posible que tenga que expandir las unidades organizativas (elija la opción▶) para encontrar la cuenta que desea.
3. En la páginaPolíticas, en la pestañaPolíticas de copia de seguridad, elijaVea la política de copia de seguridad en vigor de esta Cuenta de AWS .

   La consola muestra la directiva efectiva aplicada a la cuenta especificada.

   Note

   No puede copiar y pegar una política en vigor y usarla como JSON para otra política de copia de seguridad sin cambios significativos. los documentos de política de copia de seguridad deben incluir la propiedadOperadores de herencia (p. 98)que especifican cómo se fusiona cada configuración en la política en vigor final.

AWS CLI & AWS SDKs

Para ver la política en vigor de una cuenta

Puede utilizar uno de los siguientes comandos para ver la política de copia de seguridad en vigor:

- AWS CLI:describe-effective-policy

  En el ejemplo siguiente se muestran los detalles de una política de copia de seguridad.

```
$ aws organizations describe-effective-policy \
--policy-type BACKUP_POLICY \
--target-id 123456789012{
    "EffectivePolicy": {
        "LastUpdatedTimestamp": "2020-06-22T14:31:50.748000-07:00",
        "TargetId": "123456789012",
        "PolicyType": "BACKUP_POLICY",
        "PolicyContent": "{\"plans\":{\"pii_backup_plan\":{\"regions\":[\"ap-
northeast-2\",\"us-east-1\",\"eu-north-1\"],\
"selections\":{\"tags\":{\"datatype\":{\"iam_role_arn\":\"arn:aws:iam::$account:role/
MyIamRole\",\"tag_value\":[\"PII\"],\
"tag_key\":\"dataType\"}}},\"rules\":{\"hourly\":{\"complete_backup_window_minutes\":
\"10080\",\"target_backup_vault_name\
```

```
":\"FortKnox\",\"start_backup_window_minutes\":\"480\",\"schedule_expression\":
\"cron(0 5/1 ? * * *)\",\"lifecycle\":{\"mo
ve_to_cold_storage_after_days\":\"180\",\"delete_after_days\":\"270\"},\"copy_actions
\":{\"arn:aws:backup:us-east-1:$accou
nt:backup-vault:secondary-vault\":{\"lifecycle\":{\"move_to_cold_storage_after_days
\":\"10\",\"delete_after_days\":\"100\"
}}}}}}}}"
    }
}
```

- AWSSDK: DescribeEffectivePolicy

Ejemplos y sintaxis de políticas de copia de seguridad

En esta página se describe la sintaxis de la política de copia de seguridad y se proporcionan ejemplos.

Sintaxis de las políticas de copia de seguridad

Una política de copia de seguridad es un archivo de texto sin formato que se estructura de acuerdo con las reglas de JSON. La sintaxis de las políticas de copia de seguridad sigue la sintaxis de todos los tipos de políticas de administración. Para obtener una explicación completa de esa sintaxis, consulte Sintaxis y herencia de políticas para tipos de políticas de administración. Este tema se centra en aplicar esa sintaxis general a los requisitos específicos del tipo de política de copia de seguridad.

La mayor parte de una política de copia de seguridad es el plan de copia de seguridad y sus reglas. La sintaxis del plan de copia de seguridad dentro de una política de copia de seguridad de AWS Organizations es estructuralmente idéntica a la sintaxis utilizada por AWS Backup, pero los nombres de claves son diferentes. En las descripciones de los nombres de claves de políticas que aparecen a continuación, cada uno incluye el nombre de clave del plan de AWS Backup equivalente. Para obtener más información acerca deAWS Backupplanes, consulteCreateBackupPlanen laAWS BackupGuía para desarrolladores.

Para ser completa y funcional, una política de copia de seguridad en vigor (p. 175) debe incluir algo más que un plan de copia de seguridad con su programación y sus reglas. La política también debe identificar el Regiones de AWS y los recursos a los que se debe realizar una copia de seguridad, y elAWS Identity and Access Management(IAM) queAWS Backuppuede utilizar para realizar la copia de seguridad.

La siguiente política funcionalmente completa muestra la sintaxis básica de las políticas de copia de seguridad. Si este ejemplo se adjuntó directamente a una cuenta,AWS Backuprealizaría una copia de seguridad de todos los recursos de esa cuenta en el`us-east-1`y`eu-north-1`Regiones que tienen la etiqueta`dataType`con un valor o`PII`or`RED`. Realiza una copia de seguridad de esos recursos diariamente a las 5.00 h en `My_Backup_Vault` y también almacena una copia en `My_Secondary_Vault`. Ambos almacenes se encuentran en la misma cuenta que el recurso. También almacena una copia de la copia de seguridad en el`My_Tertiary_Vault`en una cuenta diferente, explícitamente especificada. Las bóvedas ya deben existir en cada uno de los Regiones de AWS Para cada Cuenta de AWS Que reciba la política en vigor. Si alguno de los recursos respaldados son instancias de EC2, la compatibilidad con Microsoft Volume Shadow Copy Service (VSS) está habilitada para las copias de seguridad de esas instancias. La copia de seguridad aplica la etiqueta `Owner:Backup` a cada punto de recuperación.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "rules": {
                "My_Hourly_Rule": {
                    "schedule_expression": {"@@assign": "cron(0 5 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "60"},
                    "complete_backup_window_minutes": {"@@assign": "604800"},
                    "enable_continuous_backup": {"@@assign": false},
                    "target_backup_vault_name": {"@@assign": "My_Backup_Vault"},
                    "recovery_point_tags": {
```

```
                        "Owner": {
                            "tag_key": {"@@assign": "Owner"},
                            "tag_value": {"@@assign": "Backup"}
                        }
                    },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {"@@assign": "180"},
                        "delete_after_days": {"@@assign": "270"}
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-west-2:$account:backup-
vault:My_Secondary_Vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-west-2:$account:backup-
vault:My_Secondary_Vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "180"},
                                "delete_after_days": {"@@assign": "270"}
                            }
                        },
                        "arn:aws:backup:us-east-1:$account:backup-vault:My_Tertiary_Vault":
 {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:111111111111:backup-
vault:My_Tertiary_Vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "180"},
                                "delete_after_days": {"@@assign": "270"}
                            }
                        }
                    }
                }
            },
            "regions": {
                "@@append": [
                    "us-east-1",
                    "eu-north-1"
                ]
            },
            "selections": {
                "tags": {
                    "My_Backup_Assignment": {
                        "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/
MyIamRole"},
                        "tag_key": {"@@assign": "dataType"},
                        "tag_value": {
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {
                    "windows_vss": {"@@assign": "enabled"}
                }
            },
            "backup_plan_tags": {
                "stage": {
                    "tag_key": {"@@assign": "Stage"},
                    "tag_value": {"@@assign": "Beta"}
                }
```

```
            }
        }
    }
}
```

La sintaxis de política de copia de seguridad incluye los siguientes componentes:

- `$account`variables: en ciertas cadenas de texto de las políticas, puede usar la función`$account`para representar la variable actual Cuenta de AWS . CuandoAWS BackupCuando ejecuta un plan en la política en vigor, reemplaza automáticamente esta variable por la variable actual Cuenta de AWS en el que se están ejecutando la política eficaz y sus planes.

  Important

  Puede utilizar el`$account`Solo en elementos de la política que puedan incluir un nombre de recurso de Amazon (ARN), como aquellos que especifican el almacén de copia de seguridad en el que almacenar la copia de seguridad, o el rol de IAM con permisos para realizar la copia de seguridad.

  Por ejemplo, lo siguiente requiere que un almacén denominado`My_Vault`existen en cada Cuenta de AWS A la que se aplica la política.

  ```
  arn:aws:backup:us-west-2:***$account***:vault:My_Vault"
  ```

  Recomendamos utilizarAWS CloudFormationy su integración con Organizations para crear y configurar automáticamente almacenes de copia de seguridad y roles de IAM para cada cuenta miembro de la organización. Para obtener más información, consulteCreación de un conjunto de pilas con permisos autoadministradosen laAWS CloudFormationGuía del usuario de.
- Operadores de herencia: las directivas Backup de seguridad pueden utilizar tanto la herenciaOperadores de configuración de valores (p. 99)y laOperadores de control secundarios (p. 99).
- `plans`

  En el nivel superior, la clave de la política es la clave `plans`. Una política de copia de seguridad debe comenzar siempre con este nombre de clave fijado en la parte superior del archivo de la política. Puede tener uno o más planes de copia de seguridad con esta clave.
- Cada plan con la clave de nivel superior `plans` tiene un nombre de clave que consiste en el nombre del plan de copia de seguridad asignado por el usuario. En el ejemplo anterior, el nombre del plan de copia de seguridad es `PII_Backup_Plan`. Puede tener varios planes en una política, cada uno con sus propios planes`rules`,`regions`,`selections`, y`tags`.

  Este nombre de clave del plan de copia de seguridad de una política de copia de seguridad se asigna al valor de la clave `BackupPlanName` de un plan de AWS Backup.

  Cada plan puede contener los siguientes elementos:
  - `rules (p. 179)`Esta clave contiene una colección de reglas. Cada regla se traduce en una tarea programada, con una hora de inicio y una ventana de tiempo en la que realizar la copia de seguridad de los recursos identificados por el`selections`y`regions`Elementos de la política de copia de seguridad en vigor.
  - `regions (p. 182)`— Esta clave contiene una lista de matriz de Regiones de AWS cuyos recursos pueden ser respaldados por esta política.
  - `selections (p. 182)`— Esta clave contiene una o más colecciones de recursos (dentro de la`regions`) de los que se realiza una copia de seguridad por el`rules`.
  - `advanced_backup_settings (p. 183)`— Esta clave contiene la configuración específica de las copias de seguridad que se ejecutan en determinados recursos.
  - `backup_plan_tags (p. 184)`: especifica etiquetas asociadas al plan de copia de seguridad.
- `rules`

La clave de política `rules` se asigna a la clave `Rules` de un plan de AWS Backup. Puede tener una o más reglas con la clave `rules`. Cada regla se convierte en una tarea programada para realizar una copia de seguridad de los recursos seleccionados.

Cada regla contiene una clave cuyo nombre es el nombre de la regla. En el ejemplo anterior, el nombre de la regla es “My_Hourly_Rule”. El valor de la clave de regla es la siguiente recopilación de elementos de regla:

- `schedule_expression`Esta clave de política se asigna a la`ScheduleExpression`Clave en unaAWS BackupPlan.

  Especifica la hora de inicio de la copia de seguridad. Esta clave contiene el operador de valor heredado de`@@assign` (p. 99) y un valor de cadena con una expresión CRON que especifica cuándo AWS Backup iniciará un trabajo de copia de seguridad. El formato general de la cadena CRON es: «cron ()». Cada uno es un número o comodín. Por ejemplo, `cron(0 5 ? * 1,3,5 *)` inicia la copia de seguridad a las 5.00 h todos los lunes, miércoles y viernes. `cron(0 0/1 ? * * *)` inicia la copia de seguridad cada hora a la hora, todos los días de la semana.
- `target_backup_vault_name`Esta clave de política se asigna a la`TargetBackupVaultName`Clave en unaAWS BackupPlan.

  Especifica el nombre del almacén de copia de seguridad en el que se almacenará la copia de seguridad. Para crear el valor, utilice AWS Backup. Esta clave contiene el operador de valor heredado de `@@assign` (p. 99) y un valor de cadena con un nombre de almacén.

  > **Important**
  >
  > Cuando el plan de copia de seguridad se inicia por primera vez, el almacén ya debe existir. Recomendamos utilizarAWS CloudFormationy su integración con Organizations para crear y configurar automáticamente almacenes de copia de seguridad y roles de IAM para cada cuenta miembro de la organización. Para obtener más información, consulteCreación de un conjunto de pilas con permisos autoadministradosen laAWS CloudFormationGuía del usuario de.
- `start_backup_window_minutes`Esta clave de política se asigna a la`StartWindowMinutes`Clave en unaAWS BackupPlan.

  (Opcional) Especifica el número de minutos que se deben esperar antes de cancelar un trabajo que no se inicia correctamente. Esta clave contiene el operador de valor heredado de `@@assign` (p. 99) y un valor con un número entero de minutos.
- `complete_backup_window_minutes`Esta clave de política se asigna a la`CompletionWindowMinutes`Clave en unaAWS BackupPlan.

  (Opcional) Especifica el número de minutos después de los que un trabajo de copia de seguridad se inicia correctamente antes de que deba completarse o lo canceleAWS Backup. Esta clave contiene el operador de valor heredado de `@@assign` (p. 99) y un valor con un número entero de minutos.
- `enable_continuous_backup`Esta clave de política se asigna a la`EnableContinuousBackup`Clave en unaAWS BackupPlan.

  De forma opcional, especifica siAWS Backupcrea copias de seguridad continuas.`True`CausasAWS BackupPara crear backups continuos capaces de restaurar a un momento dado (PITR).`False`(o no especificadas) causasAWS Backuppara crear copias de seguridad de instantáneas.

  > **Note**
  >
  > Debido a que las copias de seguridad habilitadas para PITR se pueden conservar durante un máximo de 35 días, debe elegir`False`o no especifique un valorifEstablezca una de las siguientes opciones:
  >
  > - Establezca`delete_after_days`a más de 35.

- Establezca`move_to_code_storage_after_days`a cualquier valor.

Para obtener más información sobre las copias de seguridad continuas, consulte.Recuperación a un momento dadoen laAWS BackupGuía para desarrolladores.

- `lifecycle`Esta clave de política se asigna a la`Lifecycle`Clave en unaAWS BackupPlan.

  (Opcional) Especifica cuándo AWS Backup traslada esta copia de seguridad al almacenamiento en frío y cuándo expira.

  - `move_to_cold_storage_after_days` Esta clave de política se asigna a la`MoveToColdStorageAfterDays`Clave en unaAWS BackupPlan.

    Especifica el número de días después de que se produzca la copia de seguridad antes de que AWS Backup mueva el punto de recuperación al almacenamiento en frío. Esta clave contiene el operador de valores de herencia de`@@assign` (p. 99) y un valor con un número entero de días.

  - `delete_after_days`Esta clave de política se asigna a la`DeleteAfterDays`Clave en unaAWS BackupPlan.

    Especifica el número de días después de que se produzca la copia de seguridad antes de que AWS Backup elimine el punto de recuperación. Esta clave contiene el operador de valores de herencia de`@@assign` (p. 99) y un valor con un número entero de días. Si realiza la transición de una copia de seguridad al almacenamiento en frío, debe permanecer allí un mínimo de 90 días, por lo que este valor debe ser un mínimo de 90 días mayor que el valor `move_to_cold_storage_after_days`.

- `copy_actions`Esta clave de política se asigna a la`CopyActions`Clave en unaAWS BackupPlan.

  (Opcional) Especifica que AWS Backup debe copiar la copia de seguridad en una o más ubicaciones adicionales. Cada ubicación de copia de seguridad se describe de la siguiente manera:

  - Clave cuyo nombre identifica de forma exclusiva esta acción de copia. En este momento, el nombre de clave debe ser el nombre de recurso de Amazon (ARN) del almacén de copia de seguridad. Esta clave contiene dos entradas.

    - `target_backup_vault_arn`Esta clave de política se asigna a la`DestinationBackupVaultArn`Clave en unaAWS BackupPlan.

      (Opcional) Especifica el almacén en el queAWS Backupalmacena una copia adicional de la copia de seguridad. El valor de esta clave contiene el`@@assign`Operador de valores herencia (p. 99)y el ARN de la bóveda.

      - Para hacer referencia a un almacén en el Cuenta de AWS en el que se está ejecutando la directiva de copia de seguridad, utilice el comando`$account`En lugar ARN número de ID de cuenta. CuandoAWS BackupCuando ejecuta el plan de copia de seguridad, reemplaza automáticamente la variable con el número de ID de cuenta de la propiedad Cuenta de AWS En el que se está ejecutando la política. Esto permite que la copia de seguridad se ejecute correctamente cuando la directiva de copia de seguridad se aplica a más de una cuenta de una organización.
      - Para hacer referencia a un almacén en un Cuenta de AWS en la misma organización, utilice el número de ID de cuenta real en el ARN.

        Important

        - Si falta esta clave, se utiliza una versión en minúsculas del ARN en el nombre de la clave principal. Debido a que los ARN distinguen entre mayúsculas y minúsculas, es posible que esta cadena no coincida con el ARN real del error y el plan falla. Por este motivo, le recomendamos que proporcione siempre esta clave y valor.
        - El almacén de copia de seguridad en el que desea copiar la copia de seguridad ya debe existir la primera vez que inicie el plan de copia de seguridad. Recomendamos utilizarAWS CloudFormationy su integración con Organizations para crear y configurar automáticamente almacenes de copia de seguridad y roles de IAM para cada cuenta

miembro de la organización. Para obtener más información, consulteCreación de un conjunto de pilas con permisos autoadministradosen laAWS CloudFormationGuía del usuario de.

- `lifecycle`Esta clave de política se asigna a la`Lifecycle`bajo la tecla`CopyAction`Clave en unaAWS BackupPlan.

  (Opcional) Especifica cuándo AWS Backup traslada esta copia de una copia de seguridad al almacenamiento en frío y cuándo expira.

  - `move_to_cold_storage_after_days` Esta clave de política se asigna a la`MoveToColdStorageAfterDays`Clave en unaAWS BackupPlan.

    Especifica el número de días después de que se produzca la copia de seguridad antes de que AWS Backup mueva el punto de recuperación al almacenamiento en frío. Esta clave contiene el operador de valores de herencia de`@@assign` (p. 99) y un valor con un número entero de días.

  - `delete_after_days`Esta clave de política se asigna a la`DeleteAfterDays`Clave en unaAWS BackupPlan.

    Especifica el número de días después de que se produzca la copia de seguridad antes de que AWS Backup elimine el punto de recuperación. Esta clave contiene el operador de valores de herencia de`@@assign` (p. 99) y un valor con un número entero de días. Si realiza la transición de una copia de seguridad al almacenamiento en frío, debe permanecer allí un mínimo de 90 días, por lo que este valor debe ser un mínimo de 90 días mayor que el valor `move_to_cold_storage_after_days`.

- `recovery_point_tags`Esta clave de política se asigna a la`RecoveryPointTags`Clave en unaAWS BackupPlan.

  (Opcional) Especifica las etiquetas que AWS Backup asocia a cada copia de seguridad que crea a partir de este plan. El valor de esta clave contiene uno o varios de los siguientes elementos:

  - Un identificador para este par de nombre de clave y valor. Este nombre para cada elemento de `recovery_point_tags` es el nombre de la clave de etiqueta en minúscula, incluso aunque la `tag_key` tenga un tratamiento de mayúsculas y minúsculas diferente. Este identificador no distingue entre mayúsculas y minúsculas. En el ejemplo anterior, este par de claves se identificó con el nombre `Owner`. Cada par de claves contiene los siguientes elementos:

    - `tag_key`: especifica el nombre de clave de etiqueta que se adjuntará al plan de copia de seguridad. Esta clave contiene el operador de valor heredado de `@@assign` (p. 99) y un valor de cadena. Este valor distingue entre mayúsculas y minúsculas.

    - `tag_value`— Especifica el valor que se adjunta al plan de copia de seguridad y que está asociado al`tag_key`. Esta clave contiene cualquiera de los operadores de valor heredado (p. 99) y uno o más valores para reemplazar, adjuntar o quitar de la política en vigor. Estos valores distinguen entre mayúsculas y minúsculas.

- `regions`

  La`regions`clave de directiva especifica qué Regiones de AWS thatAWS BackupPara encontrar los recursos que coinciden con las condiciones del archivo`selections`Clave. Esta clave contiene cualquiera de losOperadores de valor de herencia (p. 99)y uno o más valores de cadena para Región de AWS códigos, por ejemplo:`["us-east-1", "eu-north-1"]`.

- `selections`

  La clave de política `selections` especifica los recursos de los que se realiza una copia de seguridad mediante las reglas de plan de esta política. Esta clave corresponde prácticamente al objeto BackupSelection de AWS Backup. Los recursos se especifican mediante una consulta para hacer coincidir los nombres y valores de clave de etiqueta. La`selections`contiene una clave debajo de ella:`tags`.

- `tags`: especifica las etiquetas que identifican los recursos y el rol de IAM que tiene permiso para consultar los recursos y realizar una copia de seguridad de ellos. El valor de esta clave contiene uno o varios de los siguientes elementos:
  - Un identificador para este elemento de etiqueta. Este identificador de `tags` es el nombre de clave de etiqueta en minúsculas, incluso aunque la etiqueta que se consulta tiene un tratamiento de mayúsculas y minúsculas diferente. Este identificador no distingue entre mayúsculas y minúsculas. En el ejemplo anterior, se identificó un elemento con el nombre `My_Backup_Assignment`. Cada identificador de `tags` contiene los siguientes elementos:
    - `iam_role_arn`: especifica el rol de IAM que tiene permiso para acceder a los recursos identificados por la consulta de etiquetas en el cuadro de diálogo Regiones de AWS especificado por el parámetro`regions`Clave. Este valor contiene el operador de valor heredado de`@@assign` (p. 99) y un valor de cadena que contiene el ARN del rol. AWS Backup utiliza este rol para consultar y descubrir los recursos y para realizar la copia de seguridad.

      Puede usar la variable `$account` en el ARN en lugar del número de ID de cuenta. Cuando el plan de copia de seguridad es ejecutado porAWS Backup, reemplaza automáticamente la variable con el número de ID de cuenta real del Cuenta de AWS En el que se está ejecutando la política.

      > **Important**
      >
      > El rol ya debe existir cuando inicie el plan de copia de seguridad la primera vez. Recomendamos utilizarAWS CloudFormationy su integración con Organizations para crear y configurar automáticamente almacenes de copia de seguridad y roles de IAM para cada cuenta miembro de la organización. Para obtener más información, consulteCreación de un conjunto de pilas con permisos autoadministradosen laAWS CloudFormationGuía del usuario de.
    - `tag_key`— Especifica el nombre de clave de etiqueta que se va a buscar. Esta clave contiene el operador de valor heredado de `@@assign` (p. 99) y un valor de cadena. Este valor distingue entre mayúsculas y minúsculas.
    - `tag_value`— Especifica el valor que se debe asociar a un nombre de clave que coincida con`tag_key`.AWS Backupincluye el recurso en la copia de seguridad sólo si tanto el`tag_key`y`tag_value`Coincidencia. Esta clave contiene cualquiera de los operadores de valor heredado (p. 99) y uno o más valores para reemplazar, adjuntar o quitar de la política en vigor. Estos valores distinguen entre mayúsculas y minúsculas.
- `advanced_backup_settings`: especifica la configuración de escenarios de copia de seguridad específicos. Esta clave contiene una o varias opciones de configuración. Cada configuración es una cadena de objetos JSON con los siguientes elementos:
  - Nombre de clave de objeto: cadena que especifica el tipo de recurso al que se aplica la siguiente configuración avanzada.
  - Valor del objeto: cadena de objeto JSON que contiene una o más configuraciones de copia de seguridad específicas del tipo de recurso asociado.

  En este momento, la única configuración avanzada de copia de seguridad admitida habilita las copias de seguridad de Microsoft Volume Shadow Copy Service (VSS) para Windows o SQL Server que se ejecutan en una instancia de Amazon EC2. El nombre de la clave debe ser el`"ec2"`Tipo de recurso, y el valor especifica que`"windows_vss"`el soporte es`enabled`o`disabled`para las copias de seguridad realizadas en esas instancias de Amazon EC2. Para obtener más información acerca de esta característica, consulte.Creación de una Backup de seguridad de Windows habilitada para VSSen laAWS BackupGuía para desarrolladores.

```
"advanced_backup_settings": {
    "ec2": {
        "windows_vss": {
            "@@assign": "enabled"
        }
    }
```

```
}
```

- `backup_plan_tags`: especifica etiquetas asociadas al plan de copia de seguridad. Esto no afecta a las etiquetas especificadas en ninguna regla o selección.

  (Opcional) Puede asociar etiquetas a sus planes de copia de seguridad. El valor de esta clave es una colección de elementos.

  El nombre de clave de cada elemento bajo `backup_plan_tags` es el nombre de clave de etiqueta en minúsculas, incluso si la etiqueta a consultar tiene un tratamiento de caso diferente. Este identificador no distingue entre mayúsculas y minúsculas. El valor de cada una de estas entradas consta de las siguientes claves:

  - `tag_key`: especifica el nombre de clave de etiqueta que se adjuntará al plan de copia de seguridad. Esta clave contiene el operador de valor heredado de `@@assign` (p. 99) y un valor de cadena. Este valor distingue entre mayúsculas y minúsculas.
  - `tag_value`— Especifica el valor que se adjunta al plan de copia de seguridad y que está asociado al`tag_key`. Esta clave contiene el operador de valor heredado de `@@assign` (p. 99) y un valor de cadena. Este valor distingue entre mayúsculas y minúsculas.

Ejemplos de políticas de copia de seguridad

Las políticas de copia de seguridad siguientes son solo para fines informativos. En algunos de los ejemplos siguientes, el formato de espacio en blanco JSON podría comprimirse para ahorrar espacio.

Ejemplo 1: Política asignada a un nodo principal

En el ejemplo siguiente se muestra una política de copia de seguridad asignada a uno de los nodos principales de una cuenta.

Política principal: esta directiva se puede asociar a la raíz de la organización o a cualquier unidad organizativa que sea padre de todas las cuentas previstas.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@assign": [
                    "ap-northeast-2",
                    "us-east-1",
                    "eu-north-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {
                        "@@assign": "cron(0 5/1 ? * * *)"
                    },
                    "start_backup_window_minutes": {
                        "@@assign": "480"
                    },
                    "complete_backup_window_minutes": {
                        "@@assign": "10080"
                    },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {
                            "@@assign": "180"
                        },
                        "delete_after_days": {
                            "@@assign": "270"
                        }
```

```
                    },
                    "target_backup_vault_name": {
                        "@@assign": "FortKnox"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:secondary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {
                                    "@@assign": "30"
                                },
                                "delete_after_days": {
                                    "@@assign": "120"
                                }
                            }
                        },
                        "arn:aws:backup:us-west-1:111111111111:backup-
vault:tertiary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-west-1:111111111111:backup-
vault:tertiary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {
                                    "@@assign": "30"
                                },
                                "delete_after_days": {
                                    "@@assign": "120"
                                }
                            }
                        }                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": {
                            "@@assign": "arn:aws:iam::$account:role/MyIamRole"
                        },
                        "tag_key": {
                            "@@assign": "dataType"
                        },
                        "tag_value": {
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {
                    "windows_vss": {
                        "@@assign": "enabled"
                    }
                }
            }
        }
    }
}
```

Si no se heredan ni se asocian otras políticas a las cuentas, la política en vigor que se representa en cada cuenta Cuenta de AWS Es similar al ejemplo siguiente. La expresión CRON hace que la copia de seguridad se ejecute una vez por hora, a la hora en punto. El ID de cuenta 123456789012 será el ID de cuenta real de cada cuenta.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-east-1",
                "ap-northeast-3",
                "eu-north-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "lifecycle": {
                        "to_delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:
$account:vault:secondary_vault"
                            },
                            "lifecycle": {
                                "to_delete_after_days": "28",
                                "move_to_cold_storage_after_days": "180"
                            }
                        },
                        "arn:aws:backup:us-west-1:111111111111:vault:tertiary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
west-1:111111111111:vault:tertiary_vault"
                            },
                            "lifecycle": {
                                "to_delete_after_days": "28",
                                "move_to_cold_storage_after_days": "180"
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::123456789012:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {
                    "windows_vss": "enabled"
                }
            }
        }
    }
```

```
}
```

Ejemplo 2: Una política principal se fusiona con una política secundaria

En el ejemplo siguiente, una política padre heredada y una política secundaria heredada heredada o directamente asociada a un objeto Cuenta de AWS para formar la política efectiva.

Política principal— Esta directiva se puede adjuntar a la raíz de la organización o a cualquier unidad organizativa principal.

```
{
    "plans": {
       "PII_Backup_Plan": {
            "regions": { "@@append":[ "us-east-1", "ap-northeast-3", "eu-north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 0/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "60" },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "28" },
                        "to_delete_after_days": { "@@assign": "180" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign": "28" },
                                "to_delete_after_days": { "@@assign": "180" }
                            }
                        }
                    }
                },
                "selections": {
                    "tags": {
                        "datatype": {
                            "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                            "tag_key": { "@@assign": "dataType" },
                            "tag_value": { "@@assign": [ "PII", "RED" ] }
                        }
                    }
                }
        }
    }
}
```

Política de la infancia: esta política puede estar asociada directamente a la cuenta o a una unidad organizativa en cualquier nivel por debajo del que está asociada la política principal.

```
{
    "plans": {
       "Monthly_Backup_Plan": {
            "regions": {
                "@@append":[ "us-east-1", "eu-central-1" ] },
            "rules": {
                "Monthly": {
                    "schedule_expression": { "@@assign": "cron(0 5 1 * ? *)" },
```

```
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "target_backup_vault_name": { "@@assign": "Default" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "30" },
                        "to_delete_after_days": { "@@assign": "365" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:Default" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:Default"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign": "30" },
                                "to_delete_after_days": { "@@assign": "365" }
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "MonthlyDatatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyMonthlyBackupIamRole" },
                        "tag_key": { "@@assign": "BackupType" },
                        "tag_value": { "@@assign": [ "MONTHLY", "RED" ] }
                    }
                }
            }
        }
    }
}
```

Política en vigor: la política efectiva aplicada a las cuentas contiene dos planes, cada uno con su propio conjunto de reglas y conjunto de recursos a los que aplicar las reglas.

```
{
    "plans": {
       "PII_Backup_Plan": {
            "regions": [ "us-east-1", "ap-northeast-3", "eu-north-1" ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "lifecycle": {
                        "to_delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "28",
                                "to_delete_after_days": "180"
                            }
                        }
                    }
                }
            },
```

```
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [ "PII", "RED" ]
                    }
                }
            }
        },
        "Monthly_Backup_Plan": {
            "regions": [ "us-east-1", "eu-central-1" ],
            "rules": {
                "monthly": {
                    "schedule_expression": "cron(0 5 1 * ? *)",
                    "start_backup_window_minutes": "480",
                    "target_backup_vault_name": "Default",
                    "lifecycle": {
                        "to_delete_after_days": "365",
                        "move_to_cold_storage_after_days": "30"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:Default" : {
                            "target_backup_vault_arn": {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:Default"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "30",
                                "to_delete_after_days": "365"
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "monthlydatatype": {
                        "iam_role_arn": "arn:aws:iam::&ExampleAWSAccountNo3;:role/
MyMonthlyBackupIamRole",
                        "tag_key": "BackupType",
                        "tag_value": [ "MONTHLY", "RED" ]
                    }
                }
            }
        }
    }
}
```

Ejemplo 3: Una política principal evita los cambios realizados por una política secundaria

En el ejemplo siguiente, una política principal heredada utiliza los operadores de control secundarios (p. 99) para aplicar toda la configuración y evita que una política secundaria los modifique.

Política principal— Esta directiva se puede adjuntar a la raíz de la organización o a cualquier unidad organizativa principal. La presencia de `"@@operators_allowed_for_child_policies": ["@@none"]` en cada nodo de la política significa que una política secundaria no puede realizar cambios de ningún tipo en el plan. Tampoco puede una política secundaria añadir planes adicionales a la política en vigor. Esta política se convierte en la política en vigor para cada unidad organizativa y cuenta bajo la unidad organizativa a la que está asociada.

```
{
```

```
    "plans": {
        "@@operators_allowed_for_child_policies": ["@@none"],
        "PII_Backup_Plan": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "regions": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@append": [
                    "us-east-1",
                    "ap-northeast-3",
                    "eu-north-1"
                ]
            },
            "rules": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "Hourly": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "schedule_expression": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "cron(0 0/1 ? * * *)"
                    },
                    "start_backup_window_minutes": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "60"
                    },
                    "target_backup_vault_name": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "FortKnox"
                    },
                    "lifecycle": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "move_to_cold_storage_after_days": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "28"
                        },
                        "to_delete_after_days": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "180"
                        }
                    },
                    "copy_actions": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:
$account:vault:secondary_vault",
                                "@@operators_allowed_for_child_policies": ["@@none"]
                            },
                            "lifecycle": {
                                "@@operators_allowed_for_child_policies": ["@@none"],
                                "to_delete_after_days": {
                                    "@@operators_allowed_for_child_policies": ["@@none"],
                                    "@@assign": "28"
                                },
                                "move_to_cold_storage_after_days": {
                                    "@@operators_allowed_for_child_policies": ["@@none"],
                                    "@@assign": "180"
                                }
                            }
                        }
                    }
                }
            },
            "selections": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "tags": {
```

```
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "datatype": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "iam_role_arn": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "arn:aws:iam::$account:role/MyIamRole"
                        },
                        "tag_key": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "dataType"
                        },
                        "tag_value": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            },
            "advanced_backup_settings": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "ec2": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "windows_vss": {
                        "@@assign": "enabled",
                        "@@operators_allowed_for_child_policies": ["@@none"]
                    }
                }
            }
        }
    }
}
```

Política en vigor: si existe alguna directiva de copia de seguridad secundaria, se ignoran y la directiva principal se convierte en la directiva efectiva.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-east-1",
                "ap-northeast-3",
                "eu-north-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "lifecycle": {
                        "to_delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180"
                    },
                    "copy_actions": {
                        "target_backup_vault_arn": "arn:aws:backup:us-
east-1:123456789012:vault:secondary_vault",
                        "lifecycle": {
                            "move_to_cold_storage_after_days": "28",
                            "to_delete_after_days": "180"
                        }
                    }
                }
```

```
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::123456789012:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {"windows_vss": "enabled"}
            }
        }
    }
}
```

Ejemplo 4: Una política principal impide que una política secundaria realice cambios en un plan de copia de seguridad.

En el ejemplo siguiente, una política principal heredada utiliza los operadores de control secundarios (p. 99) para aplicar la configuración de un único plan y evita que una política secundaria los modifique. De todas formas, la política secundaria puede agregar planes adicionales.

Política principal— Esta directiva se puede adjuntar a la raíz de la organización o a cualquier unidad organizativa principal. Este ejemplo es similar al ejemplo anterior con todos los operadores secundarios heredados bloqueados, excepto en el nivel superior de `plans`. La configuración `@@append` en ese nivel permite a las políticas secundarias agregar otros planes a la recopilación en la política en vigor. Cualquier cambio en el plan heredado sigue bloqueado.

Las secciones del plan se truncan para mayor claridad.

```
{
    "plans": {
        "@@operators_allowed_for_child_policies": ["@@append"],
        "PII_Backup_Plan": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "regions": { ... },
            "rules": { ... },
            "selections": { ... }
        }
    }
}
```

Política de la infancia: esta política puede estar asociada directamente a la cuenta o a una unidad organizativa en cualquier nivel por debajo del que está asociada la política principal. Esta política secundaria define un nuevo plan.

Las secciones del plan se truncan para mayor claridad.

```
{
    "plans": {
        "MonthlyBackupPlan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { … }
        }
```

```
    }
}
```

Política en vigor— La política efectiva incluye ambos planes.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { ... }
        },
        "MonthlyBackupPlan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { … }
        }
    }
}
```

Ejemplo 5: Una política secundaria reemplaza la configuración de una política principal

En el ejemplo siguiente, una política secundaria utilizaOperadores de configuración de valores (p. 99)Para anular algunos de los valores heredados de una política principal.

Política principal— Esta directiva se puede adjuntar a la raíz de la organización o a cualquier unidad organizativa principal. Cualquiera de las opciones puede ser anulada por una política secundaria porque el comportamiento predeterminado, en ausencia de un operador de control secundario (p. 99) que lo impida, es permitir que la política secundaria `@@assign`, `@@append`, o `@@remove`. La política principal contiene todos los elementos necesarios para un plan de copia de seguridad válido, por lo que realiza una copia de seguridad de los recursos correctamente si se hereda tal y como está.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@append": [
                    "us-east-1",
                    "ap-northeast-3",
                    "eu-north-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {"@@assign": "cron(0 0/1 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "60"},
                    "target_backup_vault_name": {"@@assign": "FortKnox"},
                    "lifecycle": {
                        "to_delete_after_days": {"@@assign": "2"},
                        "move_to_cold_storage_after_days": {"@@assign": "180"}
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:t2": {
                            "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:vault:t2"},
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "28"},
                                "to_delete_after_days": {"@@assign": "180"}
                            }
                        }
```

```
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/
MyIamRole"},
                        "tag_key": {"@@assign": "dataType"},
                        "tag_value": {
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            }
        }
    }
}
```

Política de la infancia: la directiva secundaria incluye sólo la configuración que debe ser diferente de la directiva principal heredada. Debe haber una política principal heredada que proporcione la otra configuración necesaria cuando se fusiona en una política en vigor. De lo contrario, la política de copia de seguridad efectiva contiene un plan de copia de seguridad que no es válido y no realiza una copia de seguridad de los recursos como se esperaba.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@assign": [
                    "us-west-2",
                    "eu-central-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {"@@assign": "cron(0 0/2 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "80"},
                    "target_backup_vault_name": {"@@assign": "Default"},
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {"@@assign": "30"},
                        "to_delete_after_days": {"@@assign": "365"}
                    }
                }
            }
        }
    }
}
```

Política en vigor: la directiva efectiva incluye la configuración de ambas directivas, con la configuración proporcionada por la directiva secundaria anulando la configuración heredada del padre. En este ejemplo, se producen los siguientes cambios:

- La lista de regiones se sustituye por una lista completamente diferente. Si desea agregar una región a la lista heredada, utilice`@@append`en lugar de`@@assign`en la política de la infancia.
- AWS Backuprealiza cada dos horas en lugar de cada hora.
- AWS Backup permite que se inicie la copia de seguridad en 80 minutos en lugar de en 60 minutos.
- AWS Backup utiliza el almacén `Default` en lugar de `FortKnox`.

- El ciclo de vida se extiende tanto para la transferencia al almacenamiento en frío como para la eliminación eventual de la copia de seguridad.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-west-2",
                "eu-central-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/2 ? * * *)",
                    "start_backup_window_minutes": "80",
                    "target_backup_vault_name": "Default",
                    "lifecycle": {
                        "to_delete_after_days": "365",
                        "move_to_cold_storage_after_days": "30"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault": {
                            "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:vault:secondary_vault"},
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "28",
                                "to_delete_after_days": "180"
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            }
        }
    }
}
```

Políticas de etiquetas

Para obtener información y procedimientos comunes a todos los tipos de políticas, consulte los siguientes temas:

- Habilitar y desactivar tipos de políticas (p. 87)
- Obtenga detalles sobre las políticas (p. 90)
- Sintaxis y herencia de políticas (p. 95)

Puede utilizar políticas de etiquetas para mantener la coherencia de las etiquetas, incluido el tratamiento de casos preferentes de valores y claves de etiquetas.

¿Qué son las etiquetas?

Las etiquetas son atributos personalizados que usted o AWS asignan a los recursos de AWS. Cada etiqueta tiene dos partes:

- Una clave de etiqueta (por ejemplo, `CostCenter`, `Environment` o `Project`). Las claves de etiqueta distinguen entre mayúsculas y minúsculas.
- Un campo opcional denominado valor de etiqueta (por ejemplo, `111122223333` o `Production`). Omitir el valor de etiqueta es lo mismo que usar una cadena vacía. Al igual que las claves de etiqueta, los valores de etiqueta distinguen entre mayúsculas y minúsculas.

En el resto de esta página se describen las políticas de etiquetas. Para obtener más información acerca de las etiquetas, consulte las siguientes fuentes:

- Para obtener más información general sobre el etiquetado, incluidas las convenciones de nomenclatura y uso, consulteEtiquetadoAWSRecursosen laAWSReferencia general de.
- Para obtener una lista de los servicios que admiten el uso de etiquetas, consulte Referencia de la API de etiquetado de grupos de recursos.
- Para obtener más información acerca del etiquetado de recursos de Organizations, consulteEtiquetado de recursos de AWS Organizations (p. 229).
- Para obtener información acerca del etiquetado de recursos en otros servicios de AWS, consulte la documentación de cada uno de los servicios.
- Para obtener información acerca del uso de etiquetas para categorizar los recursos, consulte Estrategias de etiquetado de AWS.

¿Qué son las políticas de etiquetas?

Las políticas de etiquetas son un tipo de política que le puede ayudar a estandarizar las etiquetas en todos los recursos en las cuentas de su organización. En una política de etiquetas, se especifican las reglas de etiquetado aplicables a los recursos cuando se etiquetan.

Por ejemplo, una política de etiquetas puede especificar que, cuando se asocia a un recurso la etiqueta `CostCenter`, esta debe utilizar el tratamiento de mayúsculas y minúsculas y los valores de etiqueta que define la política de etiquetas. Una política de etiquetas también puede especificar que se ejecuten operaciones de etiquetado no conformes en los tipos de recursos especificados. En otras palabras, no se pueden completar las solicitudes de etiquetado no conformes en los tipos de recursos especificados. No se evalúa la conformidad con la política de etiquetas de los recursos no etiquetados o las etiquetas que no están definidas en la política de etiquetas.

El uso de políticas de etiquetas implica el uso de varios servicios de AWS:

- Utilice AWS Organizations para administrar políticas de etiquetas. Cuando inicia sesión en la cuenta de administración de la organización, utiliza Organizations para habilitar la característica de políticas de etiquetas. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización. A continuación, puede crear políticas de etiquetas y asociarlas a las entidades de la organización para poner en vigor dichas reglas de etiquetado.
- Utilice AWS Resource Groups para administrar la conformidad con las políticas de etiquetas. Cuando inicia sesión en una cuenta de su organización, utiliza Resource Groups para buscar etiquetas no conformes en los recursos de la cuenta. Puede corregir las etiquetas no conformes en el servicio de AWS donde se creara el recurso.

  Si inicia sesión en la cuenta de administración de su organización, puede ver la información de conformidad de todas las cuentas de su organización.

Las políticas de etiquetas solo están disponibles en las organizaciones que tienen todas las características habilitadas (p. 37). Para obtener más información acerca de qué se necesita para utilizar políticas de etiquetas, consulte Requisitos previos y permisos para administrar políticas de etiquetas (p. 197).

> Important
>
> Para comenzar a utilizar políticas de etiquetas, AWS recomienda encarecidamente que se siga el flujo de trabajo de ejemplo que se describe en Introducción a las políticas de etiquetas (p. 199) antes de pasar a políticas de etiquetas más avanzadas. Es mejor conocer los efectos de asociar una política de etiquetas sencilla a una única cuenta antes de ampliar las políticas de etiquetas a toda una unidad organizativa u organización. Es especialmente importante conocer los efectos de una política de etiquetas antes de ejecutar la conformidad de cualquier política de etiquetas. Las tablas de laIntroducción a las políticas de etiquetas (p. 199)También proporciona enlaces a instrucciones para tareas más avanzadas relacionadas con las políticas.

Requisitos previos y permisos para administrar políticas de etiquetas

En esta página se describen los requisitos previos y los permisos necesarios para administrar políticas de etiquetas en AWS Organizations.

Temas

- Requisitos previos para administrar políticas de etiquetas (p. 197)
- Permisos para administrar políticas de etiquetas (p. 197)

Requisitos previos para administrar políticas de etiquetas

Los requisitos para utilizar políticas de etiquetas son los siguientes:

- Su organización debe tener habilitadas todas las características (p. 37).
- Debe haber iniciado sesión en la cuenta de administración de su organización.
- Necesita los permisos que se indican en Permisos para administrar políticas de etiquetas (p. 197).

Para evaluar el cumplimiento de las políticas de etiquetas, utilice AWS Resource Groups. Para obtener información acerca de los requisitos para evaluar el cumplimiento, consulte Requisitos previos y permisos en la Guía del usuario de AWS Resource Groups.

Permisos para administrar políticas de etiquetas

En el ejemplo siguiente, la política de IAM proporciona permisos para administrar políticas de etiquetas.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageTagPolicies",
            "Effect": "Allow",
            "Action": [
                "organizations:ListPoliciesForTarget",
                "organizations:ListTargetsForPolicy",
                "organizations:DescribeEffectivePolicy",
                "organizations:DescribePolicy",
                "organizations:ListRoots",
                "organizations:DisableAWSServiceAccess",
                "organizations:DetachPolicy",
                "organizations:DeletePolicy",
```

```
                "organizations:DescribeAccount",
                "organizations:DisablePolicyType",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListPolicies",
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:EnableAWSServiceAccess",
                "organizations:ListCreateAccountStatus",
                "organizations:DescribeOrganization",
                "organizations:UpdatePolicy",
                "organizations:EnablePolicyType",
                "organizations:DescribeOrganizationalUnit",
                "organizations:AttachPolicy",
                "organizations:ListParents",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:CreatePolicy",
                "organizations:DescribeCreateAccountStatus"
            ],
            "Resource": "*"
        }
    ]
}
```

Para obtener más información acerca de las políticas y los permisos de IAM, consulteIAM User Guide.

Prácticas recomendadas para utilizar políticas de etiquetas

AWSrecomienda las siguientes prácticas para el uso de políticas de etiquetas:

Elija una estrategia de uso de mayúsculas y minúsculas en etiquetas

Determine cómo desea usar las mayúsculas y minúsculas en las etiquetas e implemente de forma coherente esa estrategia en todos los tipos de recursos. Por ejemplo, decida si se va a utilizar `Costcenter`, `costcenter` o `CostCenter` y utilice la misma convención para todas las etiquetas. Para obtener resultados coherentes en los informes de conformidad, evite utilizar etiquetas similares con un tratamiento incoherente de mayúsculas y minúsculas. Esta estrategia le ayudará a definir políticas de etiquetas para su organización.

Utilice el flujo de trabajo recomendado

Comience poco a poco creando una política de etiquetas sencilla. A continuación, asóciela a una cuenta miembro que pueda utilizar con fines de prueba. Utilice los flujos de trabajo que se describen en Introducción a las políticas de etiquetas (p. 199).

Determine las reglas de etiquetado

Esto dependerá de las necesidades de su organización. Por ejemplo, es posible que desee especificar que cuando una etiqueta `CostCenter` se asocia a secretos de AWS Secrets Manager, debe utilizar el tratamiento de mayúsculas y minúsculas especificado. Cree políticas de etiquetas que definan etiquetas conformes y asócielas a las entidades de la organización en las que desee que entren en vigor dichas reglas de etiquetado.

Forme a los administradores de la cuenta

Cuando esté listo para ampliar el uso de políticas de etiquetas, forme a los administradores de la cuenta de la siguiente manera:

- Comunique su estrategia de etiquetado.
- Haga hincapié en que los administradores han de utilizar etiquetas en tipos de recursos específicos.

  Esto es importante, ya que los recursos sin etiquetas se muestran como conformes en los resultados de conformidad.
- Proporcione instrucciones para la comprobación de la conformidad de las políticas de etiquetas. Indique a los administradores que busquen y corrijan las etiquetas no conformes en los recursos de su cuenta mediante el procedimiento que se describe en Evaluación de la conformidad de una cuenta en la Guía del usuario de AWS Resource Groups. Infórmeles de la frecuencia con la que desea que comprueben la conformidad.

Actúe con precaución al ejecutar el cumplimiento.

Forzar el cumplimiento puede impedir que los usuarios de las cuentas de su organización etiqueten los recursos que necesiten. Revise la información de Descripción de la aplicación de políticas (p. 214). Consulte también los flujos de trabajo que se describen en Introducción a las políticas de etiquetas (p. 199).

Considere la posibilidad de crear una política SCP para establecer medidas de seguridad en torno a las solicitudes de creación de recursos

Los recursos que nunca han tenido etiquetas asociadas se muestran como conformes en los informes. Los administradores de cuentas aún pueden crear recursos sin etiquetar. En algunos casos, puede utilizar una política de control de servicios (SCP) para establecer medidas de seguridad en torno a las solicitudes de creación de recursos. Para ver una SCP de ejemplo, consulte Requerir una etiqueta en los recursos creados especificados (p. 141). Para obtener información sobre si unAWSEl servicio admite el control de acceso mediante etiquetas, consulte AWSServicios que funcionan con IAMen laIAM User Guide. Busque los servicios que tengan Sí en la columna Authorization based on tags (Autorización basada en etiquetas). Elija el nombre del servicio para ver la documentación sobre la autorización y el control de acceso para dicho servicio.

Introducción a las políticas de etiquetas

El uso de políticas de etiquetas implica el uso de variasAWSServicios de . Para empezar, revise las siguientes páginas. A continuación, siga los flujos de trabajo de esta página para familiarizarse con las políticas de etiquetas y sus efectos.

- Requisitos previos y permisos para administrar políticas de etiquetas (p. 197)
- Prácticas recomendadas para utilizar políticas de etiquetas (p. 198)

Uso de políticas de etiquetas por primera vez

Siga estos pasos para comenzar a utilizar las políticas de etiquetas por primera vez.

Tarea	Cuenta en la que iniciar sesión	Consola de servicio de AWS que utilizar
Paso 1: Habilite las políticas de etiquetas de su organización. (p. 87)	La cuenta de gestión de la organización.[1]	AWS Organizations

Tarea	Cuenta en la que iniciar sesión	Consola de servicio de AWS que utilizar
Paso 2: Cree una política de etiquetas. (p. 203) Mantenga su primera política de etiquetas simple. Introduzca una clave de etiqueta en el tratamiento de mayúsculas y minúsculas que desea utilizar y deje el resto de opciones en sus valores predeterminados.	La cuenta de gestión de la organización.[1]	AWS Organizations
Paso 3: Asocie una política de etiquetas a una cuenta de miembro único que pueda utilizar para las pruebas. (p. 209) Tendrá que iniciar sesión en esta cuenta en el siguiente paso.	La cuenta de gestión de la organización.[1]	AWS Organizations
Paso 4: Cree algunos recursos con etiquetas de conformidad y otros con etiquetas no conformes.	La cuenta de miembro que está utilizando para realizar pruebas.	Cualquier servicio de AWS con el que se sienta cómodo. Por ejemplo, puede utilizar AWS Secrets Manager y seguir el procedimiento en Creación de un secreto básico para crear secretos con secretos de conformidad y no conformes.
Paso 5: Consulte la política de etiquetas en vigor y evalúe el estado de conformidad de la cuenta.	La cuenta de miembro que está utilizando para realizar pruebas.	Grupos de recursosy laAWSdonde se creó el recurso. Si ha creado recursos con etiquetas de conformidad y no conformes, debería ver las etiquetas no conformes en los resultados.
Paso 6: Repita el proceso para buscar y corregir los problemas de conformidad hasta que los recursos en la cuenta de pruebas cumplan con su política de etiquetas.	La cuenta de miembro que está utilizando para realizar pruebas.	Grupos de recursosy laAWSdonde se creó el recurso.
En cualquier momento, puede evaluar el cumplimiento en toda la organización.	La cuenta de gestión de la organización.[1]	Grupos de recursos

[1] Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.

Ampliación del uso de políticas de etiquetas

Puede realizar las siguientes tareas en cualquier orden para ampliar el uso de las políticas de etiquetas.

Tarea avanzada	Cuenta en la que iniciar sesión	Consola de servicio de AWS que utilizar
Cree políticas de etiquetas más avanzadas (p. 203). Siga el mismo proceso que para los usuarios principiantes, pero pruebe otras tareas. Por ejemplo, defina claves o valores adicionales o especifique un tratamiento de mayúsculas y minúsculas diferente para una clave de etiquetas. Puede utilizar la información en Descripción de la herencia de políticas (p. 94) y Sintaxis de la política de etiquetas (p. 223) para crear políticas de etiquetas más detalladas.	La cuenta de gestión de la organización.[1]	AWS Organizations
Asocie políticas de etiquetas a cuentas o unidades organizativas adicionales. (p. 209) Compruebe la política de etiquetas en vigor de una cuenta (p. 212) después de asociar más políticas a ella o a cualquier unidad organizativa de la que la cuenta sea miembro.	La cuenta de gestión de la organización.[1]	AWS Organizations
Cree una SCP para precisar etiquetas cuando alguien cree nuevos recursos. Para ver un ejemplo, consulte Requerir una etiqueta en los recursos creados especificados (p. 141).	La cuenta de gestión de la organización.[1]	AWS Organizations
Continúe evaluando el estado de conformidad de la cuenta con la política de etiquetas en vigor a medida que cambia. Corrija etiquetas no conformes.	Una cuenta de miembro con una política de etiquetas efectiva.	Grupos de recursosy laAWSdonde se creó el recurso.
Evalúe el cumplimiento en toda la organización.	La cuenta de gestión de la organización.[1]	Grupos de recursos

[1] Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.

Aplicación de las políticas de etiquetas por primera vez

Para aplicar políticas de etiquetas por primera vez, siga un flujo de trabajo similar al del uso de políticas de etiquetas por primera vez y utilice una cuenta de prueba.

Warning

Tenga cuidado con forzar el cumplimiento. Asegúrese de que conoce los efectos del uso de políticas de etiquetas y siga el flujo de trabajo recomendado. Pruebe el funcionamiento de la ejecución en una cuenta de prueba antes de ampliarla a más cuentas. De lo contrario, podría impedir que los usuarios de las cuentas de su organización etiqueten los recursos que necesiten. Para obtener más información, consulte Descripción de la aplicación de políticas (p. 214) .

Tareas de aplicación de políticas	Cuenta en la que iniciar sesión	Consola de servicio de AWS que utilizar
Paso 1: Cree una política de etiquetas. (p. 203) Mantenga su primera política de etiquetas aplicada simple. Introduzca una clave de etiqueta en el tratamiento de mayúsculas y minúsculas y seleccione la opción Prevent noncompliant operations for this tag (Evitar las operaciones no conformes para esta etiqueta). A continuación, especifique un tipo de recurso para aplicarlo. Continuando con nuestro ejemplo anterior, puede optar por aplicarlo en secretos de Secrets Manager.	La cuenta de gestión de la organización.[1]	AWS Organizations
Paso 2: Asocie una política de etiquetas a una única cuenta de prueba. (p. 209)	La cuenta de gestión de la organización.[1]	AWS Organizations
Paso 3: Pruebe a crear algunos recursos con etiquetas de conformidad y otros con etiquetas no conformes. No se le debería permitir crear una etiqueta de un recurso de del tipo especificado en la política de etiquetas con una etiqueta no conforme.	La cuenta de miembro que está utilizando para realizar pruebas.	Cualquier servicio de AWS con el que se sienta cómodo. Por ejemplo, puede utilizar AWS Secrets Manager y seguir el procedimiento en Creación de un secreto básico para crear secretos con secretos de conformidad y no conformes.
Paso 4: Evalúe el estado de conformidad de la cuenta con la política de etiquetas en vigor y corrija las etiquetas no conformes.	La cuenta de miembro que está utilizando para realizar pruebas.	Resource Groups y elAWSdonde se creó el recurso.
Paso 5: Repita el proceso para buscar y corregir los problemas de conformidad hasta que los recursos en la cuenta de pruebas cumplan con su política de etiquetas.	La cuenta de miembro que está utilizando para realizar pruebas.	Grupos de recursosy laAWSdonde se creó el recurso.

Tareas de aplicación de políticas	Cuenta en la que iniciar sesión	Consola de servicio de AWS que utilizar
En cualquier momento, puede evaluar el cumplimiento en toda la organización.	La cuenta de gestión de la organización.[1]	Grupos de recursos

[1] Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.

Creación, actualización y eliminación de políticas de etiquetas

En este tema:

- Después de tiHabilitar políticas de etiquetas (p. 87)para su organización, puedeCrear una política. (p. 203).
- Cuando cambien sus requisitos de etiquetado, puedePara actualizar una política existente (p. 206).
- Cuando ya no necesite una política y después de desasociarla de todas las unidades organizativas (unidades organizativas) y cuentas, puedeborrarlo (p. 209).

> **Important**
>
> Los recursos no etiquetados no aparecen como no conformes en los resultados.

Creación de una política de etiquetas

Permisos mínimos

Para crear las políticas de etiquetas, necesita permiso para ejecutar la siguiente acción:

- `organizations:CreatePolicy`

Puede crear una política de etiquetas en laAWS Management Consolede una de las dos formas siguientes:

- Un editor visual que le permite elegir opciones y generar el texto de la política JSON automáticamente.
- Un editor de texto que le permite crear directamente el texto de la política JSON usted mismo.

El editor visual facilita el proceso, pero limita su flexibilidad. Es una excelente manera de crear sus primeras políticas y sentirse cómodo al usarlas. Cuando comprenda cómo funcionan y haya comenzado a verse limitado por lo que ofrece el editor visual, puede añadir características avanzadas a sus políticas editando el texto de la política JSON usted mismo. El editor visual utiliza sólo elOperador de configuración de valores @ @assign (p. 99), y no proporciona ningún acceso a laOperadores de control secundarios (p. 99). Solo puede agregar los operadores de control secundario si edita manualmente el texto de la política JSON.

AWS Management Console

Para crear una política de etiquetas

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la página Tag policies (Políticas de etiquetas), seleccione Create policy (Crear política).
3. En la páginaCrear política, ingrese unaNombre de la políticay una opción opcionalDescripción de la política.

4. (Opcional) Puede agregar una o varias etiquetas al objeto de política en sí. Estas etiquetas no forman parte de la directiva. Para ello, elijaAñada etiquetaA continuación, introduzca una clave y un valor opcional. Dejar el valor en blanco lo establece en una cadena vacía; no es`null`. Puede adjuntar hasta 50 etiquetas a una política. Para obtener más información, consulte Etiquetado de recursos de AWS Organizations (p. 229) .
5. Puede crear la política de etiquetas mediante el Visual editor (Editor visual) como se describe en este procedimiento. También puede escribir o pegar una política de etiquetas en la pestaña JSON. Para obtener más información acerca de la sintaxis de políticas de etiquetas, consulteSintaxis de la política de etiquetas (p. 223).

   ParaNueva clave de etiqueta 1, especifique el nombre de la clave de etiqueta que desea agregar.
6. ParaEtiquetar el cumplimiento de mayúsculas, deje esta opción desactivada (la opción predeterminada) para especificar que la política de etiquetas principal heredada, si existe, debe definir el tratamiento de las mayúsculas y minúsculas en la clave de etiqueta.

   En esta política, active esta opción si desea asignar un uso específico de las mayúsculas en la clave de etiqueta. Si selecciona esta opción, el uso de mayúsculas que haya especificado enClave de etiquetaanula el tratamiento de casos especificado en una directiva padre heredada.

   Si no existe ninguna política principal y no se habilita esta opción, las claves de etiqueta con todos los caracteres en minúscula se consideran conformes. Para obtener más información acerca de la herencia de las políticas principales, consulteDescripción de la herencia de políticas (p. 94).

   > **Tip**
   >
   > Tenga en cuenta el uso de la política de etiquetas de ejemplo que se muestra en Ejemplo 1: Definir caso de clave de etiquetas en toda la organización (p. 225) como guía para crear una política de etiquetas que defina las claves de etiqueta y su tratamiento de las mayúsculas y minúsculas. Asóciela a la raíz de la organización. Posteriormente, puede crear y asociar políticas de etiquetas adicionales a las unidades organizativas o cuentas para crear reglas de etiquetado adicionales.
7. ParaCumplimiento de valores de, active esta opción si desea agregar valores permitidos para esta clave de etiqueta a cualquier valor heredado de una política principal.

   De forma predeterminada, esta opción está desactivada, lo que significa que solo se consideran conformes los valores definidos en y heredados de una política principal. Si no existe ninguna política principal y no especifica valores de etiqueta, cualquier valor (incluso la ausencia de valores) se considera conforme.

   Para actualizar la lista de valores de etiqueta aceptables, seleccioneEspecificar los valores permitidos para esta clave de etiquetay, a continuación, elijaEspecificar valores. Cuando se le soliciten, escriba los nuevos valores (un valor por cuadro) y, a continuación, elijaGuarde los cambios.
8. ParaEvitar las operaciones no conformes en esta etiqueta, le recomendamos que deje esta opción desactivada (la opción predeterminada) a menos que tenga experiencia con el uso de políticas de etiquetas. Asegúrese de haber revisado las recomendaciones enDescripción de la aplicación de políticas (p. 214), y prueba a fondo. De lo contrario, podría impedir que los usuarios de las cuentas de su organización etiqueten los recursos que necesiten.

   Si desea ejecutar la conformidad con esta clave de etiqueta, seleccione la casilla de verificación y, a continuación,Especificar tipos de recursos. Cuando se le solicite, seleccione los tipos de recursos que desea incluir en la directiva. A continuación, elija Save changes (Guardar cambios).

   > **Important**
   >
   > Al seleccionar esta opción, cualquier operación que manipule etiquetas para recursos de los tipos especificados tendrá éxito sólo si la operación da como resultado etiquetas que cumplan con la directiva.

9. (Opcional) Para agregar otra clave de etiqueta a esta política de etiquetas, elija Add tag key (Agregar clave de etiqueta). A continuación, realice los pasos 6 a 9 para definir la clave de etiqueta.
10. Cuando haya terminado de crear la política de etiquetas, elija Save changes (Guardar cambios).

AWS CLI & AWS SDKs

Para crear una política de etiquetas

Puede utilizar una de las siguientes opciones para crear una política de etiquetas:

- AWS CLI: create-policy

  Puede utilizar cualquier editor de texto para crear una política de etiquetas. Utilice la sintaxis de JSON y guarde la política de etiquetas como un archivo con cualquier nombre y extensión en una ubicación que desee. Las políticas de etiquetas pueden tener un máximo de 2500 caracteres, espacios incluidos. Para obtener más información acerca de la sintaxis de políticas de etiquetas, consulteSintaxis de la política de etiquetas (p. 223).

  Para crear una política de etiquetas

  1. Cree una política de etiquetas en un archivo de texto que tenga un aspecto similar al siguiente:

     Contenido de `testpolicy.json`:

```
{
    "tags": {
        "CostCenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            }
        }
    }
}
```

     Esta política de etiquetas define la clave de la etiqueta `CostCenter`. La etiqueta puede aceptar cualquier valor o no tener ninguno. Una política como esta significa que un recurso que tiene asociada la etiqueta CostCenter con o sin un valor es conforme.
  2. Cree una directiva que contenga el contenido de la directiva del archivo. Se ha truncado el espacio en blanco adicional en la salida para legibilidad.

```
$ aws organizations create-policy \
    --name "MyTestTagPolicy" \
    --description "My Test policy" \
    --content file://testpolicy.json \
    --type TAG_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-a1b2c3d4e5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-a1b2c3d4e5",
            "Name": "MyTestTagPolicy",
            "Description": "My Test policy",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign\":
\"CostCenter\"\n}\n}\n}\n}\n\n"
    }
```

```
}
```

- AWSSDK de en CreatePolicy

Qué hacer a continuación

Después de crear una política de etiquetas, puede poner las reglas de etiquetado en vigor. Para ello,Asociar la política (p. 209)A la raíz de la organización, las unidades organizativas (OU) Cuentas de AWS dentro de la organización o una combinación de entidades de la organización.

Actualización de una política de etiquetas

Permisos mínimos

Para actualizar una política de etiquetas, debe tener permiso para ejecutar las siguientes acciones:

- `organizations:UpdatePolicy` con un elemento `Resource` en la misma instrucción de política que incluye el ARN de la política especificada (o "*")
- `organizations:DescribePolicy` con un elemento `Resource` en la misma instrucción de política que incluye el ARN de la política especificada (o "*")

AWS Management Console

Para actualizar una política de etiquetas

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaPolíticas de etiquetaspageElija la política de etiquetas que desea actualizar.
3. Elija Edit policy (Editar política).
4. Puede introducir un nuevoNombre de la política,Descripción de la política. Puede cambiar el contenido de la política mediante elVisual editor (Editor visual)o editando elJSON.
5. Cuando haya terminado de actualizar la política de etiquetas, elija Save changes (Guardar cambios).

AWS CLI & AWS SDKs

Para actualizar una política

Puede utilizar uno de los comandos siguientes para actualizar una política:

- AWS CLI:update-policy

  En el ejemplo siguiente se cambia el nombre de una política de etiquetas.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed tag policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Type": "TAG_POLICY",
            "AwsManaged": false
```

```
        },
        "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign\":
\"CostCenter\"\n}\n}\n}\n\n"
    }
}
```

En el ejemplo siguiente se agrega o cambia la descripción de una política de etiquetas.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new tag policy description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Description": "My new tag policy description",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
       "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign\":
\"CostCenter\"\n}\n}\n}\n\n"
    }
}
```

En el siguiente ejemplo se cambia el documento de directiva JSON adjunto a una política de exclusión de servicios de IA. En este ejemplo, el contenido se toma de un archivo llamado`policy.json`con el siguiente texto:

```
{
  "tags": {
    "Stage": {
      "tag_key": {
        "@@assign": "Stage"
      },
      "tag_value": {
        "@@assign": [
          "Production",
          "Test"
        ]
      }
    }
  }
}
```

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Description": "My new tag policy description",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
```

```
        "Content": "{\"tags\":{\"Stage\":{\"tag_key\":{\"@@assign\":\"Stage\"},
\"tag_value\":{\"@@assign\":[\"Production\",\"Test\"]},\"enforced_for\":{\"@@assign
\":[\"ec2:instance\"]}}}}"
}
```

- AWSSDK de en UpdatePolicy

Edición de etiquetas adjuntas a una directiva de etiquetas

Cuando inicia sesión en la cuenta de administración de su organización, puede agregar o eliminar las etiquetas adjuntas a una política de etiquetas. Para ello, siga los pasos que se describen a continuación.

Permisos mínimos

Para editar las etiquetas adjuntas a una directiva de etiquetas en suAWSPara ello, debe contar con los siguientes permisos:

- `organizations:DescribeOrganization`(sólo consola — para navegar a la directiva)
- `organizations:DescribePolicy`(sólo consola — para navegar a la directiva)
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

Para editar las etiquetas adjuntas a una política de exclusión de servicios de IA

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaPolíticas de etiquetaspageEn la página, elija el nombre de la política con las etiquetas que desea editar.
3. En la página de detalles de la política seleccionada, elija laEtiquetasy, a continuación, elijaAdministrar etiquetas.
4. Puede realizar cualquiera de estas acciones en esta página:
   - Edite el valor de cualquier etiqueta introduciendo un nuevo valor sobre el anterior. No se puede modificar la clave. Para cambiar una clave, debe eliminar la etiqueta con la clave anterior y agregar una etiqueta con la nueva clave.
   - Elimine una etiqueta existente seleccionandoRemove.
   - Agregue una clave de etiqueta y un par de valor. SeleccionarAñada etiquetay, a continuación, introduzca el nuevo nombre de clave y el valor opcional en los cuadros proporcionados. Si deja elValorEn blanco, el valor es una cadena vacía; no es`null`.
5. SeleccionarGuarde los cambiosdespués de haber realizado todas las adiciones, eliminaciones y ediciones que desee realizar.

AWS CLI & AWS SDKs

Para editar las etiquetas asociadas a una política de etiquetas

Puede utilizar uno de los siguientes comandos para editar las etiquetas adjuntas a una política de etiquetas:

- AWS CLI:tag-resourceyuntag-resource
- AWSSDK de en TagResourceyUntagResource

Eliminación de una política de etiquetas

Cuando inicia sesión en la cuenta de administración de su organización, puede eliminar una política que ya no necesite en su organización.

Para poder eliminar una política, primero debe desasociarla de todas las entidades asociadas.

Permisos mínimos

Para eliminar una política de etiquetas, debe tener permiso para ejecutar la siguiente acción:

- `organizations:DeletePolicy`

AWS Management Console

Para eliminar una política de etiquetas

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2.
3. En la páginaPolíticas de etiquetaspageElija la política que desea eliminar.
4. En primer lugar debe desasociar la política que desea eliminar de todas las nodos raíz, unidades organizativas y cuentas. Elija el iconoimplementaciónEn la pestaña OU, elija el botón de opción situado junto a cada raíz, unidad organizativa o cuenta que se muestra en la pestañaimplementacióny, a continuación, elijaSeparar. En el cuadro de diálogo de confirmación, elijaSeparar.
5. SeleccionarEliminarEn la parte superior de la página.
6. En el cuadro de diálogo de confirmación, escriba el nombre de la política y, a continuación, elijaEliminar.

AWS CLI & AWS SDKs

Para eliminar una política de etiquetas

Puede utilizar uno de los comandos siguientes para eliminar una política:

- AWS CLI: delete-policy

  En el ejemplo siguiente se elimina la política especificada. Solo funciona si la política no está asociada a ninguna raíz, unidad organizativa o cuenta.

```
$ aws organizations delete-policy \
    --policy-id p-i9j8k7l6m5
```

  Este comando no genera ninguna salida cuando se realiza correctamente.
- AWSSDK de en DeletePolicy

Asociar y separar políticas de etiquetas

Puede utilizar las políticas de etiquetas en toda una organización además de en las unidades organizativas (OU) y las cuentas individuales.

- Cuando asocia una política de etiquetas a la raíz de su organización, la política de etiquetas se aplica a todas las cuentas y unidades organizativas de los miembros de la raíz.

- Cuando asocia una política de etiquetas a una unidad organizativa, esa política de etiquetas se aplica a las cuentas que pertenecen a la unidad organizativa. Esas cuentas también están sujetas a cualquier política de etiquetas asocia a la raíz de la organización.
- Cuando asocia una política de etiquetas a una cuenta, esa política de etiquetas se aplica a la cuenta. Además, esa cuenta está sujeta a cualquier política de etiquetas asociada a la raíz de la organización, a parte de a cualquier política de etiquetas asociada a una unidad organizativa a la que pertenece la cuenta.

La agregación de cualquier política de etiquetas que herede la cuenta, además de cualquier política de etiquetas asociada directamente a la cuenta, es la política de etiquetas en vigor (p. 212). Para obtener más información, consulte Descripción de la herencia de políticas (p. 94) .

Important

Los recursos no etiquetados no aparecen como no conformes en los resultados.

Permisos mínimos

Para asociar políticas de etiquetas, debe tener permiso para ejecutar la siguiente acción:

- `organizations:AttachPolicy`

AWS Management Console

Puede adjuntar una política de etiquetas navegando hasta la política o hasta la raíz, unidad organizativa o cuenta a la que desea adjuntar la política.

Para asociar una política de etiquetas navegando hasta la raíz, unidad organizativa o cuenta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la página Cuentas de AWS , seleccione el nombre de la raíz, unidad organizativa o cuenta a la que desea adjuntar una política. Es posible que tenga que expandir las unidades organizativas (elija la opción▶) para encontrar la unidad organizativa o la cuenta que desea.
3. En el navegadorPolíticas, en la entrada dePolíticas de etiquetas, elijaAttach.
4. Busque la política que desea y elijaAsociar política.

   La lista de políticas de etiquetas asociadas en laPolíticasse actualiza para incluir la nueva adición. El cambio de política surtirá efecto de inmediato.

Para adjuntar una directiva de etiquetas navegando a la directiva

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaPolíticas de etiquetasElija el nombre de la política que desea adjuntar.
3. En la páginaimplementaciónElija, en.Attach.
4. Elija el botón de opción situado junto a la raíz, unidad organizativa o cuenta a la que desea adjuntar la política. Es posible que tenga que expandir las unidades organizativas (elija la opción▶) para encontrar la unidad organizativa o la cuenta que desea.
5. Elija Attach policy.

   La lista de políticas de etiquetas asociadas en laimplementaciónse actualiza para incluir la nueva adición. El cambio de política surtirá efecto de inmediato.

AWS CLI & AWS SDKs

Para asociar una política de etiquetas a la raíz de la organización, la unidad organizativa o la cuenta

Puede utilizar uno de los siguientes elementos para asociar una política de etiquetas:

- AWS CLI:attach-policy

  En el siguiente procedimiento se muestra cómo asociar la política de etiquetas que acaba de crear a una única cuenta de prueba.

  - Asocie la política de etiquetas a la cuenta de prueba ejecutando un comando como el que se muestra a continuación:

    ```
    $ aws organizations attach-policy \
        --target-id <account-id> \
        --policy-id p-a1b2c3d4e5
    ```

    Este comando no tiene salida si tiene éxito.
- AWSSDK de en AttachPolicy

El cambio de política surtirá efecto de inmediato.

Qué hacer a continuación

Después de adjuntar una política de etiquetas, puede averiguar la conformidad de los recursos con esa política de etiquetas. Para ello, utilice la consola de Resource Groups. Para obtener información, consulte Evaluación de la conformidad de una cuenta en la Guía de usuario de AWS Resource Groups.

Desasociación de una política de etiquetas

Cuando inicia sesión en la cuenta de administración de su organización, puede desasociar una política de etiquetas de la raíz de la organización, unidad organizativa o cuenta a la que está asociada. Después de desasociar una política de etiquetas de una entidad, dicha política ya no se aplica a ninguna cuenta que estuviera afectada por la entidad ahora desasociada. Para desasociar una política, siga los pasos que se describen a continuación.

Permisos mínimos

Para desasociar una política de etiquetas de la raíz de una organización, unidad organizativa o cuenta, debe tener permiso para ejecutar la siguiente acción:

- `organizations:DetachPolicy`

AWS Management Console

Puede desasociar una política de etiquetas navegando hasta la política o hasta la raíz, unidad organizativa o cuenta de la que desea desasociar la política.

Para desasociar una política de etiquetas navegando hasta la raíz, unidad organizativa o cuenta a la que esté adjunta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la página Cuentas de AWS En la raíz, unidad organizativa o cuenta de la que desea desasociar una política. Es posible que tenga que expandir las unidades organizativas (elija la

opción▶) para encontrar la unidad organizativa o la cuenta que desea. Elija el nombre de la raíz, unidad organizativa o cuenta.

3. En la páginaPolíticasEn la pestaña, elija el botón de opción situado junto a la política de etiquetas que desea desasociar y, a continuación, elijaSeparar.
4. En el cuadro de diálogo de confirmación, elijaPolítica de desvinculación.

   La lista de políticas de etiquetas asociadas se actualiza. El cambio de política surtirá efecto de inmediato.

Para desasociar una directiva de etiquetas navegando hasta la directiva

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaPolíticas de etiquetasEn la página, elija el nombre de la política que desea desasociar de una raíz, unidad organizativa o cuenta.
3. En la páginaimplementación, seleccione el botón de opción situado junto a la raíz, unidad organizativa o cuenta de la que desea desasociar la política. Es posible que tenga que expandir las unidades organizativas (elija la opción▶) para encontrar la unidad organizativa o la cuenta que desea.
4. Elija Detach (Desasociar).
5. En el cuadro de diálogo de confirmación, elijaSeparar.

   La lista de políticas de etiquetas asociadas se actualiza. El cambio de política surtirá efecto de inmediato.

AWS CLI & AWS SDKs

Para desasociar una política de etiquetas de la raíz de la organización, la unidad organizativa o la cuenta

Puede utilizar uno de los siguientes elementos para desasociar una política de etiquetas:

- AWS CLI:detach-policy
- AWSSDK de en DetachPolicy

El cambio de política surtirá efecto de inmediato.

Visualización de políticas de etiquetas en vigor

Antes de comenzar a comprobar el estado de conformidad de los recursos etiquetados en una cuenta, resulta útil determinar primero la política de etiquetas en vigor para una cuenta.

¿Qué es la política de etiquetas en vigor?

La política de etiquetas en vigor especifica las reglas de etiquetado que se aplican a una cuenta. Es la agregación de cualquier política de etiquetas que herede la cuenta, además de cualquier política de etiquetas asociada directamente a la cuenta. Cuando se asocia una política de etiquetas a la raíz de la organización, esta se aplica a todas las cuentas de la organización. Cuando asocia una política de etiquetas a una unidad organizativa, esta se aplica a todas las cuentas y unidades organizativas que pertenecen a la unidad organizativa.

Por ejemplo, la política de etiquetas asociada a la raíz de la organización puede definir una`CostCenter`con cuatro valores compatibles. Una política de etiquetas diferente asociada a la cuenta puede restringir la clave `CostCenter` a solo dos de los cuatro valores compatibles. La combinación de estas políticas de etiquetas comprende la política de etiquetas en vigor. El resultado es que solo dos de los cuatro valores de etiqueta compatibles definidos en la política de etiquetas de la raíz de la organización son compatibles con la cuenta.

Para obtener más información y ejemplos más avanzados de cómo se generan políticas de etiquetas en vigor, consulte Descripción de la herencia de políticas (p. 94).

Cómo ver la política de etiquetas en vigor

Puede ver la política de etiquetas en vigor de una cuenta desde la AWS Management Console, la API de AWS o AWS Command Line Interface.

Permisos mínimos

Para ver la política de etiquetas en vigor de una cuenta, debe tener permiso para ejecutar las siguientes acciones:

- `organizations:DescribeEffectivePolicy`
- `organizations:DescribeOrganization`

AWS Management Console

Para ver la política de etiquetas en vigor de una cuenta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la página Cuentas de AWS En la página, elija el nombre de la cuenta para la que desea ver la política de etiquetas en vigor. Es posible que tenga que expandir las unidades organizativas (elija la opción▶) para encontrar la cuenta que desea.
3. En la páginaPolíticas, en la pestañaPolíticas de etiquetasEn la sección, elija.Consulte la política de etiquetas en vigor de este Cuenta de AWS .

   La consola muestra la directiva efectiva aplicada a la cuenta especificada.

   Note

   No puede copiar y pegar una política en vigor y usarla como JSON para otra política de etiquetas sin cambios significativos. Los documentos de directiva de etiquetas deben incluir elOperadores de herencia (p. 98)En el que se especifica cómo se fusiona cada configuración en la política en vigor final.

AWS CLI & AWS SDKs

Para ver la política de etiquetas en vigor de una cuenta

Puede utilizar una de las siguientes opciones para ver la política de etiquetas en vigor:

- AWS CLI:Describe-effective-policy

  Para determinar qué reglas de etiquetado se heredan o se asocian a una cuenta, ejecute la siguiente acción desde la cuenta y guarde los resultados en un archivo:

```
$ aws organizations describe-effective-policy \
```

```
    --policy-type TAG_POLICY
{
    "EffectivePolicy": {
        "PolicyContent": "{\"tags\":{\"costcenter\":{\"tag_value\":[\"*\"],\"tag_key
\":\"CostCenter\"}}}",
        "LastUpdatedTimestamp": "2020-06-09T08:34:25.103000-07:00",
        "TargetId": "123456789012",
        "PolicyType": "TAG_POLICY"
    }
}
```

Si una política de etiquetas se asocia a la cuenta, así como a la raíz o a cualquier unidad organizativa, la combinación de todas las políticas heredadas define la política de etiquetas en vigor de la cuenta. En estos casos, ejecutar`describe-effective-policy`De la cuenta devuelve el contenido combinado de todas las políticas de etiquetas de la jerarquía de la cuenta.

- AWSSDK de en DescribeEffectivePolicy

Uso de eventos de CloudWatch para monitorear etiquetas no conformes

Puede utilizar CloudWatch Events para llevar a cabo una monitorización cuando se introduzcan etiquetas no conformes. En el siguiente ejemplo de evento, el valor `"false"` de `tag-policy-compliant` indica que una nueva etiqueta no es compatible con la política de etiquetas en vigor.

```
{
  "detail-type": "Tag Change on Resource",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa"
  ],
  "detail": {
    "changed-tag-keys": [
      "a-new-key"
    ],
    "service": "ec2",
    "resource-type": "instance",
    "version": 3,
    "tag-policy-compliant": "false",
    "tags": {
      "a-new-key": "tag-value-on-new-key-just-added"
    }
  }
}
```

Puede suscribirse a eventos y especificar cadenas o patrones para monitorizarlos. Para obtener más información sobre los eventos de CloudWatch, consulteGuía del usuario de Amazon CloudWatch Events.

Descripción de la aplicación de políticas

Una política de etiquetas puede especificar que se apliquen operaciones de etiquetado no conformes en los tipos de recursos especificados. En otras palabras, no se pueden completar las solicitudes de etiquetado no conformes en los tipos de recursos especificados.

> **Important**
>
> La aplicación no afecta a los recursos que se crean sin etiquetas.

Para aplicar la conformidad de las políticas de etiquetas, realice una de las siguientes acciones al crear una política de etiquetas (p. 203):

- En la pestaña Visual editor (Editor visual), seleccione Prevent noncompliant operations for this tag (Evitar las operaciones no conformes en esta etiqueta) (p. 204).
- En la pestaña JSON, utilice el campo `enforced_for`. Para obtener información acerca de la sintaxis de políticas de etiquetas, consulte Ejemplos y sintaxis de políticas de etiquetas (p. 223).

Siga estas prácticas recomendadas para ejecutar la conformidad con las políticas de etiquetas:

- Actúe con precaución al ejecutar el cumplimiento.: asegúrese de que conoce los efectos del uso de políticas de etiquetas y siga los flujos de trabajo recomendados que se describen enIntroducción a las políticas de etiquetas (p. 199). Pruebe el funcionamiento de la ejecución en una cuenta de prueba antes de ampliarla a más cuentas. De lo contrario, podría impedir que los usuarios de las cuentas de su organización etiqueten los recursos que necesiten.
- Tenga en cuenta los tipos de recursos que puede aplicar en: solo puede imponer el cumplimiento de las directivas de etiquetas enTipos de recursos admitidos (p. 216). Se indican los tipos de recursos que admiten la ejecución de la conformidad cuando se utiliza el editor visual para crear una política de etiquetas.
- Comprender las interacciones con algunos servicios— AlgunosAWStienen agrupaciones de recursos similares a contenedores que crean recursos automáticamente para usted, y las etiquetas pueden propagarse de un recurso de un servicio a otro. Por ejemplo, las etiquetas de los grupos de Auto Scaling de Amazon EC2 y los clústeres de Amazon EMR se pueden propagar automáticamente a las instancias de Amazon EC2 que contienen. Puede contar con políticas de etiquetas para Amazon EC2 más estrictas que para los grupos de Auto Scaling o los clústeres de EMR. Si habilita la ejecución, la política de etiquetas impide que se etiqueten los recursos y puede bloquear el escalado dinámico y el aprovisionamiento.

En las secciones siguientes se muestra cómo encontrar recursos no conformes y corregirlos para que sean compatibles.

Búsqueda de recursos no conformes para una cuenta

En cada cuenta, puede obtener información acerca de los recursos no conformes. Debe ejecutar este comando desde todas las regiones en las que la cuenta tenga recursos.

Para buscar recursos no conformes para una cuenta con una política de etiquetas, puede ejecutar el siguiente comando Cuando inicie sesión en la cuenta y guarde los resultados en un archivo:

```
$ aws resourcegroupstaggingapi get-resources  --region us-east-1 \
    --include-compliance-details \
    --exclude-compliant-resources > outputfile.txt
```

Corrección de etiquetas no conformes en recursos

Después de encontrar etiquetas no conformes, realice las correcciones pertinentes mediante cualquiera de los siguientes métodos. Debe haber iniciado sesión en la cuenta que tiene el recurso con etiquetas no conformes:

- Utilice las operaciones de API de etiquetas o de la API deAWSEl servicio que creó los recursos no conformes.
- UsarAWS Resource Groups TagResourcesyUntagResourcespara añadir etiquetas que cumplan con la política en vigor o para eliminar etiquetas no conformes.

Búsqueda y corrección de problemas de no conformidad adicionales

La búsqueda y corrección de los problemas de conformidad es un proceso iterativo. Repita los pasos de las dos secciones anteriores hasta que los recursos que le importan cumplan con la política de etiquetas.

Generación de un informe de conformidad de toda la organización

En cualquier momento puede generar un informe que enumere todos los recursos etiquetados de la pestaña Cuentas de AWS en toda su organización. El informe muestra si cada recurso cumple con la política de etiquetas en vigor. Tenga en cuenta que los cambios que realice a los recursos o una política de etiquetas pueden tardar hasta 48 horas en verse reflejados en el informe de conformidad de toda la organización. Por ejemplo, supongamos que tiene una política de etiquetas que define una etiqueta estandarizada nueva para un tipo de recurso. Los recursos de ese tipo que no tienen esta etiqueta aparecen como conformes en el informe durante un máximo de 48 horas.

Puede generar el informe de la cuenta de administración de su organización en la pestaña`us-east-1`Región, siempre que tenga acceso a un bucket de Amazon S3. El bucket debe tener una política de bucket asociada como se muestra enInforme de política de bucket de Amazon S3. Para generar el informe, ejecute el siguiente comando:

```
$ aws resourcegroupstaggingapi get-compliance-summary --region us-east-1
{
    "SummaryList": [
        {
            "LastUpdated": "2020-06-09T18:40:46Z",
            "NonCompliantResources": 0
        }
    ]
}
```

Puede generar un informe a la vez.

Es posible que este informe tarde algo de tiempo en completarse. Puede comprobar su estado ejecutando el siguiente comando:

```
$ aws resourcegroupstaggingapi describe-report-creation --region us-east-1
{
    "Status": "SUCCEEDED"
}
```

Después de que el comando anterior devuelve`SUCCEEDED`Puede abrir el informe desde el bucket de Amazon S3.

Servicios y tipos de recursos que admiten la aplicación de políticas

Los siguientes servicios y tipos de recursos admiten el cumplimiento con políticas de etiquetas:

Nombre del servicio	Tipo de recurso	Sintaxis JSON
Amazon API Gateway	• Claves de API • Nombres de dominio	• `"apigateway:apikeys"` • `"apigateway:domainnames"` • `"apigateway:restapis"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
	• Operaciones de la API REST • Etapas	• `"apigateway:stages"`
AWS App Mesh	• Todos • Mesh • Enrutador • Nodo virtual • Enrutador virtual • Servicio virtual	• `"appmesh:*"` • `"appmesh:mesh"` • `"appmesh:route"` • `"appmesh:virtualNode"` • `"appmesh:virtualRouter"` • `"appmesh:virtualService"`
Amazon Athena	• Todos • Grupo de trabajo	• `"athena:*"` • `"athena:workgroup"`
AWS Backup	• Todos • Plan de copias de seguridad • Almacén	• `"backup:*"` • `"backup:backupPlan"` • `"backup:backupVault"`
AWS Certificate Manager	• Todos • Certificados	• `"acm:*"` • `"acm:certificate"`
Amazon CloudFront	• Todos • Distribución • Distribución de streaming	• `"cloudfront:*"` • `"cloudfront:distribution"` • `"cloudfront:streaming-distribution"`
AWS CloudTrail	• Todos • Trail	• `"cloudtrail:*"` • `"cloudtrail:trail"`
Amazon CloudWatch	• Todos • Alarma	• `"cloudwatch:*"` • `"cloudwatch:alarm"`
Amazon CloudWatch Events	• Todos • Bus de eventos • Rule	• `"events:*"` • `"events:event-bus"` • `"events:rule"`
Amazon CloudWatch Logs	• Todos • Grupo de registros	• `"logs:*"` • `"logs:log-group"`
AWS CodeBuild	• Todos • Previsión	• `"codebuild:*"` • `"codebuild:project"`
AWS CodeCommit	• Todos • Repositorio	• `"codecommit:*"` • `"codecommit:repository"`
AWS CodePipeline	• Todos • Tipo de acción • Canalización • Webhook	• `"codepipeline:*"` • `"codepipeline:actiontype"` • `"codepipeline:pipeline"` • "codepipeline:webhook"

Nombre del servicio	Tipo de recurso	Sintaxis JSON
Amazon Cognito Identity	• Todos • Grupo de identidades	• `"cognito-identity:*"` • `"cognito-identity:identitypool"`
Amazon Cognito user pools	• Todos • Grupo de usuarios	• `"cognito-idp:*"` • `"cognito-idp:userpool"`
Amazon Comprehend	• Todos • Clasificador de documentos • Reconocedor de entidades	• `"comprehend:*"` • `"comprehend:document-classifier"` • `"comprehend:entity-recognizer"`
AWS Config	• Todos • Autorización de agregación • Agregador de configuración • Regla de configuración	• `"config:*"` • `"config:aggregation-authorization"` • `"config:config-aggregator"` • `"config:config-rule"`
AWS Database Migration Service	• Todos • punto de enlace • ES • Rep. • Subgrp • Tarea	• `"dms:*"` • `"dms:endpoint"` • `"dms:es"` • `"dms:rep"` • `"dms:subgrp"` • `"dms:task"`
AWS Direct Connect	• Todos • Dxcon • Dxlag • Dxvif	• `"directconnect:*"` • `"directconnect:dxcon"` • `"directconnect:dxlag"` • `"directconnect:dxvif"`
Amazon DynamoDB	• Todos • Tabla	• `"dynamodb:*"` • `"dynamodb:table"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
Amazon EC2	• Reserva de capacidad • Punto de enlace de Client VPN • Gateway de cliente • Opciones de DHCP • Elastic IP • Flota • Imagen FPGA • Reserva de alojamiento • Imagen • Instancia • Gateway de Internet • Plantilla de lanzamiento • gateway NAT • ACL de red • Interfaz de red • Reserved Instances • Tabla de ruteo • Security group (Grupo de seguridad) • Instantánea • Solicitud de instancia de spot • Subred • Filtro de reflejo de tráfico • Sesión de reflejo de tráfico • Destino de reflejo de tráfico • Volumen • VPC • Punto de conexión VPC • Servicio de punto de enlace de la VPC • Interconexión de VPC • conexión de VPN • gateway VPN	• `"ec2:capacity-reservation"` • `"ec2:client-vpn-endpoint"` • `"ec2:customer-gateway"` • `"ec2:dhcp-options"` • `"ec2:elastic-ip"` • `"ec2:fleet"` • `"ec2:fpga-image"` • `"ec2:host-reservation"` • `"ec2:image"` • `"ec2:instance"` • `"ec2:internet-gateway"` • `"ec2:launch-template"` • `"ec2:natgateway"` • `"ec2:network-acl"` • `"ec2:network-interface"` • `"ec2:reserved-instances"` • `"ec2:route-table"` • `"ec2:security-group"` • `"ec2:snapshot"` • `"ec2:spot-instance-request"` • `"ec2:subnet"` • `"ec2:traffic-mirror-filter"` • `"ec2:traffic-mirror-session"` • `"ec2:traffic-mirror-target"` • `"ec2:volume"` • `"ec2:vpc"` • `"ec2:vpc-endpoint"` • `"ec2:vpc-endpoint-service"` • `"ec2:vpc-peering-connection"` • `"ec2:vpn-connection"` • `"ec2:vpn-gateway"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
AWS Elastic Beanstalk	• Aplicación • Versión de la aplicación • Plantilla de configuración • Plataforma	• `"elasticbeanstalk:application"` • `"elasticbeanstalk:applicationversion"` • `"elasticbeanstalk:configurationtemplate"` • `"elasticbeanstalk:platform"`
Amazon Elastic Container Service	• Clúster • Servicio • Conjunto de tareas	• `"ecs:cluster"` • `"ecs:service"` • `"ecs:task-set"`
Amazon Elastic File System	• Todos • Sistema de archivos	• `"elasticfilesystem:*"` • `"elasticfilesystem:file-system"`
Amazon EMR	• Todos • Clúster • Editor	• `"elasticmapreduce:*"` • `"elasticmapreduce:cluster"` • `"elasticmapreduce:editor"`
Amazon ElastiCache	• Clúster	• `"elasticache:cluster"`
Elastic Load Balancing	• Todos • Balanceador de carga • Grupo de destinos	• `"elasticloadbalancing:*"` • `"elasticloadbalancing:loadbalancer"` • `"elasticloadbalancing:targetgroup"`
Amazon FSx	• Todos • Copia de seguridad • Sistema de archivos	• `"fsx:*"` • `"fsx:backup"` • `"fsx:file-system"`
AWS IoT Analytics	• Todos • Canal • Conjunto de datos • Almacén de datos • Canalización	• `"iotanalytics:*"` • `"iotanalytics:channel"` • `"iotanalytics:dataset"` • `"iotanalytics:datastore"` • `"iotanalytics:pipeline"`
AWS IoT Events	• Todos • Modelo de detector • Input	• `"iotevents:*"` • `"iotevents:detectorModel"` • `"iotevents:input"`
AWS Key Management Service	• Todos • Key	• `"kms:*"` • `"kms:key"`
Amazon Kinesis	• Todos • Aplicación	• `"kinesisanalytics:*"` • `"kinesisanalytics:application"`
Amazon Kinesis Data Firehose	• Todos • Flujo de entrega	• `"firehose:*"` • `"firehose:deliverystream"`
AWS Lambda	• Todos • Función	• `"lambda:*"` • `"lambda:function"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
Amazon RDS	• Grupo de parámetros del clúster • Suscripción a eventos • Grupo de opciones de base de datos • DB Parameter Group (Grupo de parámetros de base de datos) • Instancia de base de datos reservada • Grupo de seguridad de base de datos • Grupo de subred de base de datos	• `"rds:cluster-pg"` • `"rds:es"` • `"rds:og"` • `"rds:pg"` • `"rds:ri"` • `"rds:secgrp"` • `"rds:subgrp"`
Amazon Redshift	• Todos • Clúster • Grupo de base de datos • Nombre de base de datos • Usuario de base de datos • Suscripción a eventos • Certificado de cliente del HSM • Configuración del HSM • Grupo de parámetros • Instantánea • Autorización de copia de snapshot • Programación de instantáneas • Subnet group	• `"redshift:*"` • `"redshift:cluster"` • `"redshift:dbgroup"` • `"redshift:dbname"` • `"redshift:dbuser"` • `"redshift:eventsubscription"` • `"redshift:hsmclientcertificate"` • `"redshift:hsmconfiguration"` • `"redshift:parametergroup"` • `"redshift:snapshot"` • `"redshift:snapshotcopygrant"` • `"redshift:snapshotschedule"` • `"redshift:subnetgroup"`
AWS Resource Access Manager	• Todos • Uso compartido de recursos	• `"ram:*"` • `"ram:resource-share"`
AWS Resource Groups	• Todos • Grupo	• `"resource-groups:*"` • `"resource-groups:group"`
Amazon Route 53	• Zona hospedada	• `"route53:hostedzone"`
Amazon Route 53 Resolver	• Todos • Punto de enlace de solucionador • Regla de solucionador	• `"route53resolver:*"` • `"route53resolver:resolver-endpoint"` • `"route53resolver:resolver-rule"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
Amazon S3	• Bucket	• `"s3:bucket"`
Amazon SageMaker	• Todos • Trabajo de entrenamiento • Trabajo de procesamiento • Grupo de paquetes de modelos de • UI de tareas humanas • Acción • Canalización • Experimento • Previsión	• `"sagemaker:*"` • `"sagemaker:training-job"` • `"sagemaker:processing-job "` • `"sagemaker:model-package-group"` • `"sagemaker:human-task-ui"` • `"sagemaker:action"` • `"sagemaker:pipeline"` • `"sagemaker:experiment"` • `"sagemaker:project"`
AWS Secrets Manager	• Todos • secreta	• `"secretsmanager:*"` • `"secretsmanager:secret"`
Amazon Simple Notification Service (SNS)	• Todos • Tema	• `"sns:*` • `"sns:topic"`
Amazon Simple Queue Service (SQS)	• Queue	• `"sqs:queue"`
AWS Step Functions	• Actividad	• `"states:activity"`
AWS Storage Gateway	• Todos • Gateway • Share • Cinta • Volumen	• `"storagegateway:*"` • `"storagegateway:gateway"` • `"storagegateway:share"` • `"storagegateway:tape"` • `"storagegateway:volume"`
AWS Systems Manager	• Ejecución de automatización • Document • Tarea de la ventana de mantenimiento • Instancia administrada • Elemento de operaciones • Base de referencia de parches • Session	• `"ssm:automation-execution"` • `"ssm:document"` • `"ssm:maintenancewindowtask"` • `"ssm:managed-instance"` • `"ssm:opsitem"` • `"ssm:patchbaseline"` • `"ssm:session"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
Amazon WorkSpaces	• Todos • Directorio • WorkSpace • Paquete de WorkSpaces • Imagen de WorkSpaces • Grupo IP de WorkSpaces	• `"workspaces:*"` • `"workspaces:directory"` • `"workspaces:workspace"` • `"workspaces:workspacebundle"` • `"workspaces:workspaceimage"` • `"workspaces:workspaceipgroup"`

Ejemplos y sintaxis de políticas de etiquetas

En esta página se describe la sintaxis de la política de etiquetas y se proporcionan ejemplos.

Sintaxis de la política de etiquetas

Una política de etiquetas es un archivo de texto sin formato que se estructura de acuerdo con las reglas de JSON. La sintaxis de las políticas de etiquetas sigue la sintaxis de los tipos de políticas de administración. Para obtener una discusión completa de esa sintaxis, consulteSintaxis y herencia de políticas para tipos de políticas de administración (p. 97). En este tema se centra en aplicar esa sintaxis general a los requisitos específicos del tipo de política de etiquetas.

La siguiente política de etiquetas muestra una sintaxis de política de etiquetas básica:

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "100",
                    "200"
                ]
            },
            "enforced_for": {
                "@@assign": [
                    "secretsmanager:*"
                ]
            }
        }
    }
}
```

La sintaxis de políticas de etiquetas incluye los siguientes elementos:

- El nombre de clave del campo `tags`. Las políticas de etiquetas siempre comienzan con este nombre de clave fijo. Es la línea superior del ejemplo de política anterior.
- Una clave de política que identifica únicamente a la declaración de política. Debe coincidir con el valor de la clave de etiqueta, excepto en el tratamiento de mayúsculas y minúsculas. A diferencia de la clave de etiqueta (que se describe a continuación), el valor de políticano esSensibilidad de mayúsculas

  En este ejemplo, `costcenter` es la clave de política.

- Al menos una clave de etiqueta que especifica la clave de etiqueta permitida con el uso de mayúsculas que desea que cumplan los recursos. Si no se define el tratamiento de mayúsculas y minúsculas, las minúsculas son el tratamiento predeterminado para las claves de etiqueta. El valor de la clave de etiqueta debe coincidir con el valor de la clave de política. No obstante, dado que el valor de la clave de política no distingue entre mayúsculas y minúsculas, el uso de mayúsculas puede ser diferente.

  En este ejemplo, `CostCenter` es la clave de etiqueta. Este es el tratamiento de mayúsculas y minúsculas que se requiere para conformidad con la política de etiquetas. Los recursos con tratamiento alternativo de mayúsculas y minúsculas para esta clave de etiqueta no son compatibles con la política de etiquetas.

  Puede definir varias claves de etiqueta en una política de etiquetas.
- (Opcional) Una lista de uno o varios valores de etiqueta aceptables para la clave de etiqueta. Si la política de etiquetas no especifica un valor de etiqueta para una clave de etiqueta, cualquier valor (incluso si no existe ninguno) se considera conforme.

  En este ejemplo, los valores aceptables para la clave de etiqueta `CostCenter` son `100` y `200`.
- (Opcional) Una opción `enforced_for` que indica si se debe evitar o no cualquier operación de etiquetado no conforme en los recursos y los servicios especificados. En la consola, es la opción Prevent noncompliant operations for this tag (Evitar las operaciones no conformes en esta etiqueta) del editor visual para crear políticas de etiquetas. La configuración predeterminada para esta opción es nula.

  El ejemplo de política de etiquetas especifica que todos los recursos de AWS Secrets Manager deben tener esta etiqueta.

  > Warning
  >
  > Únicamente tiene que cambiar esta opción de configuración predeterminada si tiene experiencia en el uso de políticas de etiquetas. De lo contrario, podría evitar que los usuarios de las cuentas de la organización creen los recursos que necesitan.
- Operadores que especifican cómo se combina la política de etiquetas con las otras políticas de etiquetas del árbol de organización para crear una política de etiquetas en vigor (p. 212) de la cuenta. En este ejemplo, se utiliza `@@assign` para asignar cadenas a `tag_key`, `tag_value` y `enforced_for`. Para obtener más información acerca de los operadores, consulte Operadores de herencia (p. 98).
- : Puede utilizar el`*`Comodín en los valores de etiquetas y`enforced_for`.
  - Puede utilizar sólo un comodín por valor de etiqueta. Por ejemplo, `*@example.com` está permitido, pero `*@*.com` no.
  - Para `enforced_for`, puede utilizar `<service>:*` con algunos servicios para habilitar la aplicación de todos los recursos de ese servicio. Para obtener una lista de los servicios y tipos de recursos compatibles `enforced_for`, consulte Servicios y tipos de recursos que admiten la aplicación de políticas (p. 216).

    No puede utilizar un comodín para especificar todos los servicios ni para especificar un recurso para todos los servicios.

Ejemplos de políticas de etiquetas

Las políticas de etiquetas (p. 195) siguientes son solo para fines informativos.

> Note
>
> Antes de intentar usar estos ejemplos de políticas de etiquetas en la organización, tenga en cuenta lo siguiente:
>
> - Asegúrese de que ha seguido el flujo de trabajo recomendado (p. 199) para comenzar con las políticas de etiquetas.

- Debería revisar y personalizar cuidadosamente estas políticas de etiquetas según sus requisitos únicos.
- Todos los caracteres de la política de etiquetas están sujetos a un tamaño máximo (p. 330). Los ejemplos que aparecen en esta guía muestran las políticas de etiquetas formateadas con espacios en blanco adicionales para mejorar su legibilidad. Sin embargo, para ahorrar espacio si el tamaño de política se acerca al tamaño máximo, puede eliminar cualquier espacio en blanco. Entre los ejemplos de espacio en blanco se incluyen caracteres de espacio y saltos de línea que están fuera de comillas.
- Los recursos no etiquetados no aparecen como no conformes en los resultados.

Ejemplo 1: Definir caso de clave de etiquetas en toda la organización

En el ejemplo siguiente se muestra una política de etiquetas que solo define dos claves de etiqueta y el uso de mayúsculas en los que desea que las cuentas de su organización se estandarice.

Directiva A: directiva de etiqueta raíz de la organización

```
{
    "tags": {
        "CostCenter": {
            "tag_key": {
                "@@assign": "CostCenter",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        },
        "Project": {
            "tag_key": {
                "@@assign": "Project",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        }
    }
}
```

Esta política de etiquetas define dos claves de etiquetas `CostCenter` y `Project`. La asociación de esta política de etiquetas a la raíz de la organización tiene los siguientes efectos:

- Todas las cuentas de su organización heredan esta política de etiquetas.
- Todas las cuentas de su organización deben utilizar el tratamiento de mayúsculas y minúsculas definido para conformidad. Los recursos con `CostCenter` y `Project` etiquetas cumplen los requisitos. Los recursos con tratamiento de mayúsculas y minúsculas alternativo para la clave de etiqueta (por ejemplo `costcenter`, `Costcenter` o `COSTCENTER`) no cumplen los requisitos.
- Las líneas de `@@operators_allowed_for_child_policies": ["@@none"]` bloquean las claves de etiquetas. Las políticas de etiquetas que se asocian más abajo en el árbol de organización (políticas secundarias) no pueden utilizar operadores de configuración de valores para los cambios de la clave de etiquetas, incluido el tratamiento de mayúsculas y minúsculas.
- Como ocurre con todas las políticas de etiquetas, no se evalúa la conformidad con la política de etiquetas de los recursos no etiquetados o las etiquetas que no están definidas en la política de etiquetas.

AWS recomienda que utilice este ejemplo como guía para crear una política de etiquetas similar para las claves de etiquetas que desee utilizar. Asóciela a la raíz de la organización. A continuación, cree una política de etiquetas similar al siguiente ejemplo, que solo define los valores aceptables para las claves de etiqueta definidas.

Paso siguiente: Definir valores

Suponga que asoció la política de etiquetas anterior a la raíz de la organización. A continuación, puede crear una política de etiquetas como la siguiente y asociarla a una cuenta. Esta política define valores aceptables para las claves de etiquetas `CostCenter` y `Project`.

Directiva B: directiva de etiqueta de cuenta

```
{
    "tags": {
        "CostCenter": {
            "tag_value": {
                "@@assign": [
                    "Production",
                    "Test"
                ]
            }
        },
        "Project": {
            "tag_value": {
                "@@assign": [
                    "A",
                    "B"
                ]
            }
        }
    }
}
```

Si asocia la política A a la raíz de la organización y la política B a una cuenta, las políticas se combinan para crear la siguiente política de etiquetas efectiva para la cuenta:

Política A + política B = política de etiquetas en vigor para la cuenta

```
{
    "tags": {
        "Project": {
            "tag_value": [
                "A",
                "B"
            ],
            "tag_key": "Project"
        },
        "CostCenter": {
            "tag_value": [
                "Production",
                "Test"
            ],
            "tag_key": "CostCenter"
        }
    }
}
```

Para obtener más información acerca de la herencia de políticas, además de ejemplos acerca de cómo funcionan los operadores de herencia y ejemplos de políticas de etiquetas en vigor, consulte Descripción de la herencia de políticas (p. 94).

Ejemplo 2: Evitar el uso de una clave de etiqueta

Para evitar el uso de una clave de etiqueta, puede asociar una política de etiquetas como la siguiente a una entidad de organización.

Esta política de ejemplo especifica que no se aceptan valores para la clave de etiqueta `Color`. También especifica que no se permiten operadores (p. 98) en las políticas de etiquetas secundarias. Por lo tanto, se considera que las etiquetas de `Color` de los recursos de las cuentas afectadas no cumplen los requisitos. Sin embargo, el`enforced_for`En realidad, impide que las cuentas afectadas etiquetenSoloTablas de Amazon DynamoDB con`Color`etiqueta.

```
{
    "tags": {
        "Color": {
            "tag_key": {
                "@@operators_allowed_for_child_policies": [
                    "@@none"
                ],
                "@@assign": "Color"
            },
            "tag_value": {
                "@@operators_allowed_for_child_policies": [
                    "@@none"
                ],
                "@@assign": []
            },
            "enforced_for": {
                "@@assign": [
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

Regiones admitidas

Las características de la política de etiquetas están disponibles en las siguientes regiones:

Nombre de la región	Parámetro de la región
US East (Ohio) Region	`us-east-2`
Región EE.UU. Este (Virginia) [1]	**`us-east-1`**
US West (N. California) Region	`us-west-1`
US West (Oregon) Region	`us-west-2`
Región[2] África (Ciudad del Cabo)	`af-south-1`
Región Asia-Pacífico (Hong Kong)	`ap-east-1`
Asia Pacific (Mumbai) Region	`ap-south-1`
Región Asia-Pacífico (Osaka)	`ap-northeast-3`
Asia Pacific (Seoul) Region	`ap-northeast-2`
Asia Pacific (Singapore) Region	`ap-southeast-1`
Asia Pacific (Sydney) Region	`ap-southeast-2`
Asia Pacific (Tokyo) Region	`ap-northeast-1`
Región Asia-Pacífico (Osaka)	`ap-northeast-3`

Nombre de la región	Parámetro de la región
Canada (Central) Region	`ca-central-1`
Europe (Frankfurt) Region	`eu-central-1`
Región Europa (Milán)	`eu-south-1`
Europe (Ireland) Region	`eu-west-1`
Europe (London) Region	`eu-west-2`
Región de Europa (París)	`eu-west-3`
Región Europa (Estocolmo)	`eu-north-1`
Región Oriente Medio (Baréin)	`me-south-1`
South America (São Paulo) Region	`sa-east-1`

[1] Debe especificar la**`us-east-1`**Región cuando llame a las siguientes operaciones de Organizations:

- DeletePolicy
- DisablePolicyType
- EnablePolicyType
- Cualquier otra operación en la raíz de una organización, como ListRoots.

También debe especificar la**`us-east-1`**Región cuando llame a las siguientes operaciones de la API de etiquetado de Resource Groups que forman parte de la característica de políticas de etiquetas:

- DescribeReportCreation
- GetComplianceSummary
- GetResources
- StartReportCreation

> **Note**
>
> Para evaluar el cumplimiento de políticas de etiquetas en toda la organización, también debe tener acceso a un bucket de de Amazon S3 en la región de EE.UU. Este (Norte de Virginia) para el almacenamiento de informes. Para obtener más información, consulteInforme de política de bucket de Amazon S3.

[2]Estas regiones deben estar habilitadas manualmente. Para obtener más información acerca de la activación y desactivación Regiones de AWS , consulteAdministración Regiones de AWS en laAWSReferencia general de. La consola de Resource Groups no está disponible en estas regiones.

Etiquetado de recursos de AWS Organizations

Una etiqueta es una designación de atributo personalizada que añade a un recurso de AWS para facilitar la identificación, la organización y la búsqueda de recursos. Cada etiqueta tiene dos partes:

- Una clave de etiqueta (por ejemplo, `CostCenter`, `Environment` o `Project`). Las claves de etiqueta pueden tener una longitud de hasta 128 caracteres y distinguen mayúsculas y minúsculas.
- Un valor de etiqueta (por ejemplo, `111122223333` o `Production`). Los valores de etiqueta pueden tener una longitud de hasta 256 caracteres y, como las claves de etiqueta, distinguen entre mayúsculas y minúsculas. Puede establecer el valor de una etiqueta como una cadena vacía, pero no puede asignarle un valor nulo. Omitir el valor de etiqueta es lo mismo que usar una cadena vacía.

Para obtener más información acerca de los caracteres permitidos en una clave o valor de etiqueta, consulte la sección Parámetro Tags de la API de etiquetas en la Referencia de la API de etiquetado para Resource Groups.

Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Para obtener más información, consulte Estrategias de etiquetado de AWS.

> Tip
>
> Usar Políticas de etiquetas (p. 195) Para ayudar a estandarizar la implementación de etiquetas en todos los recursos de las cuentas de su organización.

En la actualidad, AWS Organizations admite las siguientes operaciones de etiquetado cuando inicia sesión en la cuenta de administración:

- Puede añadir etiquetas a los siguientes recursos de la organización:
  - Cuentas de AWS
  - Unidades organizativas
  - La raíz de la organización
  - Políticas

Puede agregar etiquetas en los siguientes momentos:

- Al crear el recurso (p. 230): especifique las etiquetas en la consola Organizations o utilice la herramienta `Tags` con uno de los parámetros `CreateOperaciones` de la API de. Esto no es aplicable a la raíz de la organización.
- Después de crear el recurso (p. 230)— Utilice la consola Organizations o llame al método `TagResource`.

Puede ver las etiquetas en cualquiera de los recursos etiquetables en AWS Organizations Para ello, utilice la consola de o llamando a la `ListTagsForResource`.

Puede eliminar etiquetas de un recurso especificando las claves que desea eliminar mediante la consola de o llamando a la `UntagResource`.

Uso de etiquetas

Las etiquetas le ayudan a organizar sus recursos, ya que le permiten agruparlos por cosas según las categorías que le sean útiles. Por ejemplo, puede asignar una etiqueta «Departamento» que realice el seguimiento del departamento propietario. Puede asignar una etiqueta «Entorno» para rastrear si un recurso determinado forma parte de sus entornos alfa, beta, gamma o producción.

- Puede hacer lo siguienteaplicar normas de etiquetado en los recursos mediante directivas de etiquetas (p. 195).
- Las etiquetas le pueden ayudar acontrolar quién puede acceder y administrar los componentes que componen su organización (p. 318).

Agregar, actualizar y quitar etiquetas

Cuando inicia sesión en la cuenta de administración de su organización, puede añadir etiquetas a los recursos de su organización.

Agregar etiquetas a un recurso cuando lo crea

Permisos mínimos

Para añadir etiquetas a un recurso cuando lo crea, debe tener los siguientes permisos:

- Permiso para crear un recurso del tipo especificado
- `organizations:TagResource`
- `organizations:ListTagsForResource`: solo se requiere cuando se utiliza la consola Organizations

Puede incluir claves y valores de etiqueta asociados a los siguientes recursos a medida que los crea.

- Cuenta de AWS
  - Creada la cuenta (p. 63)
  - Cuenta invitada (p. 55)
- unidad organizativa (p. 79)
- Política
  - Política de exclusión de servicios de IA (p. 146)
  - Política Backup (p. 165)
  - Política de control de servicios (p. 111)
  - Política de etiquetas (p. 203)

La raíz de la organización se crea al crear inicialmente la organización, por lo que sólo puede agregarle etiquetas como un recurso existente.

Agregar o actualizar etiquetas para un recurso existente

También puede agregar nuevas etiquetas o actualizar los valores de las etiquetas asociadas a recursos existentes.

Permisos mínimos

Para añadir o actualizar etiquetas a los recursos de su organización, necesita los siguientes permisos:

- `organizations:TagResource`
- `organizations:ListTagsForResource`: solo se requiere cuando se utiliza la consola Organizations

Para quitar etiquetas de los recursos de su organización, necesita los siguientes permisos:

- `organizations:UntagResource`

AWS Management Console

Para añadir, actualizar o quitar etiquetas de un recurso existente

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. Desplácese hasta la cuenta, raíz, unidad organizativa o política y haga clic en su nombre para abrir su página de detalles.
3. En la pestaña Tags (Etiquetas), elija Manage tags (Administrar etiquetas).
4. Puede añadir nuevas etiquetas, modificar los valores de etiquetas existentes o quitar etiquetas.

   Para añadir una etiqueta, elijaAñadir etiquetay, a continuación, escriba unClave dey, opcionalmente, unValorPara la etiqueta.

   Para quitar una etiqueta, elija Remove (Quitar).

   Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas. Utilice el uso de mayúsculas que desee definir como estándar. También debe cumplir con los requisitos de las directivas de etiquetas que se apliquen.
5. Repita el paso anterior tantas veces como necesite.
6. Elija Save changes (Guardar cambios).

AWS CLI & AWS SDKs

Para añadir o actualizar etiquetas a un recurso existente

Puede utilizar uno de los siguientes comandos para añadir etiquetas a los recursos etiquetables de su organización:

- AWS CLI:tag-resource
- AWSSDK de. TagResource

Para eliminar etiquetas de un recurso de la organización

Puede utilizar uno de los siguientes comandos para eliminar etiquetas:

- AWS CLI:untag-resource
- AWSSDK de. UntagResource

Uso de AWS Organizations con otros servicios de AWS.

Puede utilizarAcceso de confianzapara habilitar unAWSque especifique, llamadoservicio de confianzaPara realizar tareas en su organización y en sus cuentas en su nombre. Esto implica conceder permisos al servicio de confianza, peronode lo contrario, afectan a los permisos para los usuarios o roles de IAM. Cuando se habilita el acceso, el servicio de confianza puede crear una función de IAM denominadaRol vinculado al servicio deen todas las cuentas de su organización siempre que se necesite ese rol. Este rol tiene una política de permisos que permite al servicio de confianza realizar las tareas que se describen en la documentación del servicio. Esto le permite especificar las opciones y los detalles de configuración que desea que el servicio de confianza mantenga en las cuentas de la organización en su nombre. El servicio de confianza solo crea roles vinculados al servicio cuando necesita realizar acciones de administración en cuentas, y no necesariamente en todas las cuentas de la organización.

Important

werecomienda encarecidque habilite y deshabilite el acceso de confianza medianteSolola consola del servicio de confianza o suAWS CLIo equivalentes de operación API. Esto permite al servicio de confianza realizar cualquier inicialización necesaria al habilitar el acceso de confianza, como la creación de los recursos necesarios y la limpieza necesaria de los recursos al deshabilitar el acceso de confianza.
Para obtener información acerca de cómo habilitar o deshabilitar el acceso a servicios de confianza a su organización mediante el servicio de confianza, consulte laMás informaciónEn elAdmite el acceso de confianzaen la columnaServicios de AWS que se pueden utilizar con AWS Organizations (p. 237).
Si deshabilita el acceso mediante la consola de Organizations, los comandos de CLI o las operaciones de API, se producen las siguientes acciones:

- El servicio ya no puede crear una función vinculada al servicio en las cuentas de su organización. Esto significa que el servicio no puede realizar operaciones en su nombre en ninguna cuenta nueva de su organización. El servicio aún puede realizar operaciones en cuentas antiguas hasta que el servicio complete su limpieza desdeAWS Organizations.
- El servicio ya no puede realizar tareas en las cuentas de miembro de la organización, a menos que esas operaciones estén explícitamente permitidas por las directivas de IAM asociadas a sus roles. Esto incluye cualquier agregación de datos de las cuentas de miembro a la cuenta de administración o a una cuenta de administrador delegada, cuando proceda.
- Algunos servicios detectan esto y limpian los datos o recursos restantes relacionados con la integración, mientras que otros servicios dejan de acceder a la organización pero dejan los datos históricos y la configuración para permitir una posible reactivación de la integración.

En su lugar, el uso de la consola o comandos del otro servicio para deshabilitar la integración garantiza que el otro servicio pueda limpiar los recursos necesarios sólo para la integración. La forma en que el servicio limpia sus recursos en las cuentas de la organización depende de ese servicio. Para obtener más información, consulte la documentación deAWSservicio de.

Permisos necesarios para habilitar el acceso de confianza

El acceso de confianza requiere permisos para dos servicios: AWS Organizations y el servicio de confianza. Para habilitar el acceso de confianza, elija uno de los escenarios siguientes:

- Si tiene credenciales con permisos enAWS OrganizationsY el servicio de confianza, habilite el acceso mediante las herramientas (la consola o laAWS CLI) proporcionada por el servicio de confianza. Esto permite al servicio habilitar el acceso de confianza enAWS OrganizationsEn su nombre, así como crear todos los recursos que necesita para funcionar en su organización.

  Los permisos mínimos para estas credenciales son los siguientes:

  - `organizations:EnableAWSServiceAccess`. También puede utilizar la`organizations:ServicePrincipal`Con esta operación para limitar las solicitudes que esas operaciones realizan a una lista de nombres de principal de servicio aprobados. Para obtener más información, consulte Claves de condición (p. 310) .
  - `organizations:ListAWSServiceAccessForOrganization`: obligatorio si se utiliza elAWS Organizationsconsola de .
  - Los permisos mínimos necesarios que requiere el servicio de confianza dependen del servicio. Para obtener más información, consulte la documentación del servicio de confianza.
- Si una persona tiene credenciales con permisos en AWS Organizations, pero otra persona tiene credenciales con permisos en el servicio de confianza, siga estos pasos en el orden que se indica a continuación:
  1. La persona que tiene credenciales con permisos en AWS Organizations debe utilizar la consola de AWS Organizations, la AWS CLI de o un SDK de AWS para habilitar el acceso de confianza del servicio de confianza. Esto concederá permiso al otro servicio para llevar a cabo la configuración necesaria en la organización cuando se realice el siguiente paso (paso 2).

     Los permisos mínimos de AWS Organizations son los siguientes:

     - `organizations:EnableAWSServiceAccess`
     - `organizations:ListAWSServiceAccessForOrganization`: obligatorio solo si se utiliza elAWS Organizationsconsole

     Para conocer los pasos para habilitar el acceso de confianza en AWS Organizations, consulte Cómo habilitar o deshabilitar el acceso de confianza (p. 234).
  2. La persona que tiene credenciales con permisos en el servicio de confianza habilita ese servicio para trabajar con AWS Organizations. Esto indica al servicio que debe realizar todas las inicializaciones necesarias, como la creación de los recursos necesarios para que el servicio de confianza funcione en la organización. Para obtener más información, consulte las instrucciones específicas de los servicios en Servicios de AWS que se pueden utilizar con AWS Organizations (p. 237).

Permisos necesarios para deshabilitar el acceso de confianza

Si ya no desea permitir que el servicio de confianza realice tareas en la organización o en las cuentas de esta, elija uno de los escenarios siguientes.

> Important
>
> La deshabilitación del acceso del servicio de confianza no impide que los usuarios y los roles con los permisos apropiados utilicen dicho servicio. Para bloquear completamente a los usuarios y roles el acceso a unaAWS, puede quitar los permisos de IAM que otorgan ese accesoEn el caso de, puede utilizarPolíticas de control de servicios (SCP) (p. 108)inAWS Organizations.
> Puede aplicar SCP a solo cuentas miembro. Los SCP no se aplican a la cuenta de administración. Le recomendamos que utiliceno ejecuten servicios en la cuenta de administración. (p. 25) En su lugar, ejecútelos en cuentas de miembros donde puede controlar la seguridad mediante SCP.

- Si tiene credenciales con permisos tanto en AWS Organizations como en el servicio de confianza, deshabilite el acceso utilizando las herramientas (la consola o la AWS CLI) disponibles para el servicio

de confianza. A continuación, el servicio realiza una limpieza eliminando los recursos que ya no son necesarios y deshabilitando el acceso de confianza del servicio en AWS Organizations en su nombre.

Los permisos mínimos para estas credenciales son los siguientes:

- `organizations:DisableAWSServiceAccess`. También puede utilizar la`organizations:ServicePrincipal`Con esta operación para limitar las solicitudes que esas operaciones realizan a una lista de nombres de principal de servicio aprobados. Para obtener más información, consulte Claves de condición (p. 310) .
- `organizations:ListAWSServiceAccessForOrganization`: obligatorio si se utiliza elAWS Organizationsconsola de .
- Los permisos mínimos necesarios que requiere el servicio de confianza dependen del servicio. Para obtener más información, consulte la documentación del servicio de confianza.

- Si las credenciales que tienen permisos en AWS Organizations no coinciden con las credenciales que tienen permisos en el servicio de confianza, siga estos pasos en el orden que se indica a continuación:
  1. La persona con permisos en el servicio de confianza primero deshabilita el acceso utilizando dicho servicio. Esto indica al servicio de confianza que debe eliminar los recursos necesarios para el acceso de confianza. Para obtener más información, consulte las instrucciones específicas de los servicios en Servicios de AWS que se pueden utilizar con AWS Organizations (p. 237).
  2. La persona con permisos en AWS Organizations podrá entonces utilizar la consola de AWS Organizations, la AWS CLI de o un SDK de AWS para deshabilitar el acceso del servicio de confianza. Esto eliminará los permisos para el servicio de confianza de la organización y las cuentas de esta.

     Los permisos mínimos de AWS Organizations son los siguientes:

     - `organizations:DisableAWSServiceAccess`
     - `organizations:ListAWSServiceAccessForOrganization`: obligatorio solo si se utiliza elAWS Organizationsconsole

     Para conocer los pasos para deshabilitar el acceso de confianza en AWS Organizations, consulte Cómo habilitar o deshabilitar el acceso de confianza (p. 234).

Cómo habilitar o deshabilitar el acceso de confianza

Si solo tiene permisos para AWS Organizations y desea habilitar o deshabilitar el acceso de confianza a la organización en nombre del administrador del otro servicio de AWS, utilice el siguiente procedimiento.

Important

werecomienda encarecidque habilite y deshabilite el acceso de confianza medianteSolola consola del servicio de confianza o suAWS CLIo equivalentes de operación API. Esto permite al servicio de confianza realizar cualquier inicialización necesaria al habilitar el acceso de confianza, como la creación de los recursos necesarios y la limpieza necesaria de los recursos al deshabilitar el acceso de confianza.
Para obtener información acerca de cómo habilitar o deshabilitar el acceso a servicios de confianza a su organización mediante el servicio de confianza, consulte laMás informaciónEn elAdmite el acceso de confianzaen la columnaServicios de AWS que se pueden utilizar con AWS Organizations (p. 237).
Si deshabilita el acceso mediante la consola de Organizations, los comandos de CLI o las operaciones de API, se producen las siguientes acciones:

- El servicio ya no puede crear una función vinculada al servicio en las cuentas de su organización. Esto significa que el servicio no puede realizar operaciones en su nombre en ninguna cuenta nueva de su organización. El servicio aún puede realizar operaciones en cuentas antiguas hasta que el servicio complete su limpieza desdeAWS Organizations.

- El servicio ya no puede realizar tareas en las cuentas de miembro de la organización, a menos que esas operaciones estén explícitamente permitidas por las directivas de IAM asociadas a sus roles. Esto incluye cualquier agregación de datos de las cuentas de miembro a la cuenta de administración o a una cuenta de administrador delegada, cuando proceda.
- Algunos servicios detectan esto y limpian los datos o recursos restantes relacionados con la integración, mientras que otros servicios dejan de acceder a la organización pero dejan los datos históricos y la configuración para permitir una posible reactivación de la integración.

En su lugar, el uso de la consola o comandos del otro servicio para deshabilitar la integración garantiza que el otro servicio pueda limpiar los recursos necesarios sólo para la integración. La forma en que el servicio limpia sus recursos en las cuentas de la organización depende de ese servicio. Para obtener más información, consulte la documentación deAWSservicio de.

AWS Management Console

Para habilitar el acceso al servicio de confianza

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaServiciosEn el caso de, busque la fila del servicio que desea habilitar y elija su nombre.
3. Elija Habilitar acceso de confianza.
4. En el cuadro de diálogo de confirmación, marque la casillaMostrar la opción para habilitar el acceso de confianza, introduzca**`enable`**En el cuadro y, a continuación, elija.Para habilitar el acceso de confianza.
5. Si va a habilitar el acceso, dígale al administrador del otro servicio de AWS que ahora puede habilitar el otro servicio para que funcione con AWS Organizations.

Para deshabilitar el acceso del servicio de confianza

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaServiciosEn el caso de, busque la fila del servicio que desea deshabilitar y elija su nombre.
3. Espere hasta que el administrador del otro servicio le indique que el servicio está deshabilitado y que sus recursos se han eliminado.
4. En el cuadro de diálogo de confirmación, introduzca**`disable`**En el cuadro y, a continuación, elija.Deshabilitar el acceso de confianza.

AWS CLI, AWS API

Para habilitar o deshabilitar el acceso del servicio de confianza

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para habilitar o deshabilitar el acceso del servicio de confianza:

- AWS CLI:AWSOrganizationsenable-aws-service-access
- AWS CLI:AWSOrganizationsdisable-aws-service-access
- API de AWS: EnableAWSServiceAccess
- API de AWS: DisableAWSServiceAccess

AWS Organizations y roles vinculados al servicio

AWS OrganizationsutilizaFunciones vinculadas al servicio de IAMPara permitir que los servicios de confianza realicen tareas en su nombre en las cuentas miembro de su organización. Al configurar un servicio de confianza y autorizar su integración con la organización, dicho servicio puede solicitar que AWS Organizations cree una función vinculada a sí mismo en su cuenta miembro. El servicio de confianza realiza acción de forma asíncrona según lo necesite, pero no necesariamente en todas las cuentas de la organización al mismo tiempo. La función vinculada al servicio tiene permisos de IAM predefinidos que permiten al servicio de confianza realizar solo tareas específicas en esa cuenta. En general, AWS administra todas las funciones vinculadas a servicios, lo que significa que normalmente no puede modificar las funciones ni las políticas adjuntas.

Para que todo esto sea posible, al crear una cuenta en una organización o aceptar una invitación para unir su cuenta existente a una organización,AWS Organizationsaprovisiona la cuenta miembro con una función vinculada al servicio denominada`AWSServiceRoleForOrganizations`. Solo el propio servicio AWS Organizations puede asumir esta función. El rol tiene permisos que permitenAWS OrganizationsPara crear roles vinculados al servicio para otrosAWSServicios de . Este rol vinculado a un servicio está presente en todas las organizaciones.

Aunque no lo recomendamos, si su organización tiene solo las características de facturación unificada (p. 7) habilitadas, el rol vinculado a un servicio denominado `AWSServiceRoleForOrganizations` no se utiliza nunca y puede eliminarlo. Si más adelante desea habilitar todas las características (p. 7) de la organización, el rol es necesario y debe restaurarlo. Las siguientes comprobaciones se producen cuando inicia el proceso para habilitar todas las características:

- Para cada cuenta de miembro que seinvitado a unirseorganización: el administrador de la cuenta recibe una solicitud para que acepte la habilitación de todas las características. Para aceptar correctamente la solicitud, el administrador debe tener los permisos `organizations:AcceptHandshake` e `iam:CreateServiceLinkedRole` si el rol vinculado a un servicio (`AWSServiceRoleForOrganizations`) no existe todavía. Si el rol `AWSServiceRoleForOrganizations` ya existe, el administrador necesita únicamente el permiso `organizations:AcceptHandshake` para aceptar la solicitud. Si no existe una función vinculada al servicio, AWS Organizations la crea cuando el administrador acepta la solicitud.
- Para cada cuenta de miembro que secreatedEn la organización: el administrador de la cuenta recibe una solicitud para volver a crear el rol vinculado al servicio. (El administrador de la cuenta miembro no recibe una solicitud para habilitar todas las funciones, ya que el administrador de la cuenta administración (anteriormente conocida como la «cuenta maestra») se considera el propietario de las cuentas miembro creadas).AWS Organizationscrea el rol vinculado a un servicio cuando el administrador de la cuenta miembro acepta la solicitud. El administrador debe tener los permisos `organizations:AcceptHandshake` e `iam:CreateServiceLinkedRole` para aceptar correctamente el protocolo de enlace.

Después de habilitar todas las características de su organización, ya no puede eliminar el rol vinculado al servicio `AWSServiceRoleForOrganizations` de cualquier cuenta.

> **Important**
>
> Las SCP de AWS Organizations nunca afectan a las funciones vinculadas a servicios. Estos roles están exentos de cualquier restricción de las SCP.

Servicios de AWS que se pueden utilizar con AWS Organizations

conAWS OrganizationsPuede realizar actividades de administración de cuentas a escala mediante la consolidación de varios Cuentas de AWS en una sola organización. La consolidación de cuentas simplifica la forma de utilizar otros servicios de AWS. Puede aprovechar los servicios de administración de varias cuentas en AWS Organizations con servicios seleccionados de AWS para realizar tareas en todas las cuentas que son miembros de su organización.

En la siguiente tabla se muestran los servicios de AWS que puede utilizar con AWS Organizations y el beneficio de utilizar cada servicio en toda una organización.

Acceso de confianza— Puede habilitar unAWSpara realizar operaciones en todos los Cuentas de AWS En su organización, Para obtener más información, consulte Uso de AWS Organizations con otros servicios de AWS. (p. 232) .

Administrador delegadoUn compatibleAWSpuede registrar unAWSen la organización como administrador de las cuentas de la organización en ese servicio.

AWSServicio de	Beneficios de uso con AWS Organization	Admite el acceso de confianza	Admite administradores delegados	
AWS Artifact (p. 256) Descargue informes de seguridad y conformidad de AWS, como los informes ISO y PCI.	Puede aceptar acuerdos en nombre de todas las cuentas de su organización.	Sí Más información (p. 257)	No	
AWS Audit Manager (p. 259) Automatice la recopilación continua de pruebas para ayudarle a auditar el uso de los servicios en la nube.	Audit de forma continua suAWSutilizar en varias cuentas de su organización para simplificar la forma en que evalúa el riesgo y el cumplimiento.	Sí Más información (p. 259)	Sí Más información (p. 261)	
AWS Backup (p. 261) Administre y supervise	Puede configurar y administrar planes de copias de	Sí Más información (p. 262)	No	

AWSServicio de	Beneficios de uso con AWS Organization	Admite el acceso de confianza	Admite administradores delegados	
las copias de seguridad de todas las cuentas de su organización.	seguridad de toda la organización o de grupos de cuentas de las unidades organizativas (OU). Puede supervisar las copias de seguridad de todas sus cuentas de manera centralizada.			
AWS CloudFormation Conjuntos de pilas de (p. 263) Cree, actualice o elimine pilas de varias cuentas y regiones en una sola operación.	Un usuario de la cuenta de administración o una cuenta de administrador delegado puede crear un conjunto de pilas con permisos administrados por servicios que implemente instancias de pila en cuentas de su organización.	Sí Más información (p. 264)	Sí Más información (p. 265)	

AWSServicio de	Beneficios de uso con AWS Organization	Admite el acceso de confianza	Admite administradores delegados	
AWS CloudTrail (p. 265) Habilite la auditoría de riesgos y operaciones, el gobierno y la conformidad de su cuenta.	Un usuario en una cuenta de administración puede crear un registro de seguimiento de la organización que registre todos los eventos de todas las cuentas de dicha organización.	Sí Más información (p. 266)	No	
Amazon CloudWatch Events Monitoree sus recursos deAWS y las aplicaciones que ejecuta en AWS en tiempo real.	Puede habilitar el uso compartido de todos los eventos de CloudWatch en todas las cuentas de su organización. Para obtener más información, consulteEnvío y recepción de eventos entre Cuentas de AWS en laGuía del usuario de Amazon CloudWatch Events.	No	No	

AWSServicio de	Beneficios de uso con AWS Organization	Admite el acceso de confianza	Admite administradores delegados	
AWS Compute Optimizer (p. 268) Obtenga recomendaciones de optimización informática de AWS.	Puede analizar todos los recursos que se encuentran en las cuentas de su organización para obtener recomendaciones de optimización. Para obtener más información, consulteCuentas admitidas por Compute Optimizeren laAWS Compute OptimizerGuía del usuario de.	Sí Más información (p. 270)	No	

AWSServicio de	Beneficios de uso con AWS Organization	Admite el acceso de confianza	Admite administradores delegados	
AWS Config (p. 270) Evalúe, audite y analice las configuraciones de sus recursos de AWS.	Puede obtener una vista de toda la organización del estado de conformidad. También puede utilizarAWS ConfigOperaciones de la APIAdministraciónAWS Configreglas y paquetes de conformidad en todos los Cuentas de AWS En su organización, Puede utilizar una cuenta de administrador delegada para agregar la configuración de recursos y los datos de conformidad de todas las cuentas miembros de una organización enAWS Organizations. Para obtener más información, consulteRegistro de un administrador delegadoen la AWS	Sí Más información (p. 272)	Sí Más información: Reglas de configuración Paquetes de conformidad Acumulación de datos de varias cuentas y regiones	

AWSServicio de	Beneficios de uso con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	Config Guía para desarrolladores de .			

AWSServicio de	Beneficios de uso con AWS Organization	Admite el acceso de confianza	Admite administradores delegados	
AWS Control Tower Configure y controle una cuenta que sea segura, cumpla con las normas correspondientesAWSMedio ambiente.	Puede establecer una landing zone, un entorno con varias cuentas para todos losAWSde AWS. Este entorno incluye una organización y entidades de organización. Puede utilizar este entorno para aplicar regulaciones de conformidad en todos los Cuentas de AWS . Para obtener más información, consulte Cómo funciona AWS Control Tower y Administrar cuentas a través de AWS Organizations en la Guía del usuario de AWS Control Tower.	Sí Más información	No	

AWSServicio de	Beneficios de uso con AWS Organization	Admite el acceso de confianza	Admite administradores delegados	
AWS Directory Service (p. 272) Configure y ejecute directorios en la nube de AWS o conecte los recursos de AWS a una instancia de Microsoft Active Directory existente en las instalaciones.	Puede integrar AWS Directory Service con AWS Organizations para compartir los directorios sin interrupciones entre varias cuentas y en cualquier VPC de una región.	Sí Más información (p. 273)	No	
AWS Firewall Manager (p. 274) Configure y administre de forma centralizada las reglas de firewall para las aplicaciones web en sus cuentas y aplicaciones.	Puede configurar y administrar de manera centralizada AWS WAF Reglas de en todas las cuentas de su organización.	Sí Más información (p. 274)	Sí Más información (p. 276)	

AWSServicio de	Beneficios de uso con AWS Organization	Admite el acceso de confianza	Admite administradores delegados	
Amazon GuardDuty (p. 277) GuardDuty es un servicio de monitorización continua de la seguridad que analiza y procesa la información de una variedad de fuentes de datos. Utiliza fuentes de información de amenazas y aprendizaje automático para identificar la actividad inesperada y potencialmente no permitida, así como la actividad malintencionada en suAWSMedio ambiente.	Puede designar una cuenta de miembro para ver y administrar GuardDuty para todas las cuentas de su organización. Agregar cuentas miembro habilita automáticamente GuardDuty para las cuentas en el Región de AWS . También puede automatizar la activación de GuardDuty para nuevas cuentas agregadas a su organización. Para obtener más información, consulteGuardDuty y Organizationsen laGuía del usuario de Amazon GuardDuty.	Sí Más información (p. 277)	Sí Más información (p. 278)	

AWSServicio de	Beneficios de uso con AWS Organization	Admite el acceso de confianza	Admite administradores delegados	
AWS Health (p. 279) Obtenga visibilidad de los eventos que pueden afectar a los problemas de rendimiento o disponibilidad de los recursos paraAWSServicios de .	Puede agregarAWS HealthEventos en todas las cuentas de su organización.	Sí Más información (p. 279)	No	

AWSServicio de	Beneficios de uso con AWS Organization	Admite el acceso de confianza	Admite administradores delegados	
AWS Identity and Access Management Controle de forma segura el acceso a los recursos de AWS.	Puede utilizarPara los datos de los últimos servicioseN IAM para ayudarle a comprender mejorAWSen toda la organización. Puede utilizar estos datos para crear y actualizar las políticas de control del servicio (SCP) (p. 108) que restringen el acceso únicamente a los servicios de AWS que utilizan las cuentas de su organización. Para ver un ejemplo, consulte .Uso de datos para ajustar los permisos de una unidad organizativaen laGuía del usuario de IAM	No	No	

AWSServicio de	Beneficios de uso con AWS Organization	Admite el acceso de confianza	Admite administradores delegados	
IAM Access Analyzer Analice las políticas basadas en recursos en suAWSpara identificar las políticas que concedan acceso a una entidad principal fuera de su zona de confianza.	Puede designar una cuenta miembro para que sea administrador de IAM Access Analyzer. Para obtener más información, consulteHabilitación del Access Analyzeren laIAM User Guide.	Sí Más información	Sí Más información	
AWS License Manager (p. 281) Simplifique el proceso de transferencia de las licencias de software a la nube.	Puede habilitar el descubrimiento entre cuentas de recursos informáticos en toda su organización.	Sí Más información (p. 282)	Sí Más información (p. 283)	

AWSServicio de	Beneficios de uso con AWS Organization	Admite el acceso de confianza	Admite administradores delegados	
Amazon Macie (p. 283) Descubre y clasifica el contenido crítico para su empresa mediante el aprendizaje automático para ayudarle a cumplir los requisitos de privacidad y seguridad de datos. Evalúa continuamente el contenido almacenado en Amazon S3 y le notifica posibles problemas.	Puede configurar Amazon Macie para todas las cuentas de su organización para obtener una vista consolidada de todos sus datos en Amazon S3, en todas las cuentas desde una cuenta de administrador de Macie designada. Puede configurar Macie para proteger automáticamente los recursos de las cuentas nuevas a medida que crece la organización. Se le alerta para corregir las configuraciones de política incorrectas en los buckets de S3 de toda la organización.	Sí Más información (p. 284)	Sí Más información (p. 285)	

AWSServicio de	Beneficios de uso con AWS Organization	Admite el acceso de confianza	Admite administradores delegados	
AWS Marketplace (p. 285) es un catálogo digital seleccionado que puede utilizar para buscar, comprar, implementar y administrar software, datos y servicios de terceros que necesita para desarrollar soluciones y hacer funcionar sus negocios.	Puede compartir licencias para su AWS Marketplace Suscripciones y compras en las cuentas de su organización.	Sí Más información (p. 286)	No	

AWSServicio de	Beneficios de uso con AWS Organization	Admite el acceso de confianza	Admite administradores delegados	
AWS Resource Access Manager (p. 287) Comparta recursos de AWS específicos de su propiedad con otras cuentas.	Puede compartir recursos dentro de su organización sin intercambiar invitaciones adicionales. Entre los recursos que puedes compartir se incluyenReglas de resolución de Route 53, reservas de capacidad bajo demanda y mucho más. Para obtener información acerca de cómo compartir reservas de capacidad, consulte laGuía del usuario de Amazon EC2 para instancias de Linuxo elGuía del usuario de Amazon EC2 para instancias de Windows. Para obtener	Sí Más información (p. 288)	No	

AWSServicio de	Beneficios de uso con AWS Organization	Admite el acceso de confianza	Admite administradores delegados	
	una lista de los recursos compartibles, consulteRecursos compartiblesen laAWS RAMGuía del usuario de.			
AWS Security Hub (p. 290) Consulte su estado de seguridad enAWSy contrastar su entorno con los estándares y las prácticas recomendadas del sector de la seguridad.	Puede habilitar automáticamente Security Hub para todas las cuentas de su organización, incluidas las cuentas nuevas a medida que se agregan. Esto aumenta la cobertura de las comprobaciones y hallazgos de Security Hub, lo que proporciona una imagen más precisa de su postura general de seguridad.	Sí Más información (p. 291)	Sí Más información (p. 291)	

AWSServicio de	Beneficios de uso con AWS Organization	Admite el acceso de confianza	Admite administradores delegados	
Amazon S3 Storage Lens (p. 291) Obtenga visibilidad de sus métricas de actividad y uso del almacenamiento de Amazon S3 con recomendaciones prácticas para optimizar el almacenamiento.	Configure Amazon S3 Storage Lens para obtener visibilidad de las tendencias de actividad y uso del almacenamiento de Amazon S3, así como de recomendaciones para todas las cuentas de miembros de su organización.	Sí Más información (p. 292)	Sí Más información (p. 293)	
AWS Service Catalog (p. 294) Cree y administre catálogos de servicios de TI aprobados para su uso en AWS.	Puede compartir carteras de productos y copiar productos entre cuentas con más facilidad, sin necesidad de compartir los ID de cartera de productos.	Sí Más información (p. 294)	Sí Más información	

AWSServicio de	Beneficios de uso con AWS Organization	Admite el acceso de confianza	Admite administradores delegados	
Service Quotas (p. 297) Consulte y administre sus cuotas de servicio, también conocidas como límites, desde una ubicación central.	Puede crear una plantilla de solicitud de cuota para solicitar automáticamente un aumento de cuotas cuando se creen las cuentas de su organización.	Sí Más información (p. 297)	No	
AWS Single Sign-On (p. 298) Proporcione servicios de inicio de sesión único para todas sus cuentas y aplicaciones en la nube.	Los usuarios pueden iniciar sesión en elAWS SSOCon sus credenciales corporativas y acceder a recursos en su cuenta de administración asignada o en sus cuentas de miembro.	Sí Más información (p. 298)	No	

AWSServicio de	Beneficios de uso con AWS Organization	Admite el acceso de confianza	Admite administradores delegados	
AWS Systems Manager (p. 300) Obtenga control y visibilidad de sus recursos de AWS.	Puede sincronizar los datos de las operaciones en todas las Cuentas de AWS en su organización mediante el Explorador de Systems Manager. Puede administrar plantillas de cambios, aprobaciones e informes para todas las cuentas de miembros de su organización desde una cuenta de administrador delegada mediante Systems Manager Change Manager.	Sí (sólo el Explorador de Systems Manager) Más información (p. 301)	Sí Más información (p. 303)	

AWSServicio de	Beneficios de uso con AWS Organization	Admite el acceso de confianza	Admite administradores delegados	
Políticas de etiquetas (p. 304) Utilice las etiquetas de estandarizar en los recursos de las cuentas de su organización.	Puede crear políticas de etiquetas para definir las reglas de etiquetado para recursos y tipos de recursos específicos, y asociar dichas políticas a unidades organizativas y cuentas para hacer cumplir las reglas.	Sí Más información (p. 304)	No	
AWS Trusted Advisor (p. 305) Trusted AdvisorInspeccione elAWSy realiza recomendaciones cuando surge la oportunidad de ahorrar dinero, mejorar el desempeño y la disponibilidad del sistema o ayudar a cerrar los errores de seguridad.	Ejecución deTrusted Advisorcomprueba todos los Cuentas de AWS En su organización,	Sí Más información (p. 306)	No	

AWS Artifact y AWS Organizations

AWS Artifact es un servicio que le permite descargar informes de seguridad y conformidad de AWS, como informes ISO y PCI. Uso deAWS ArtifactMediante, un usuario de la cuenta de administración de la organización puede aceptar acuerdos automáticamente en nombre de todas las cuentas miembro de una organización, incluso cuando se añadan nuevos informes y cuentas. Los usuarios de las cuentas miembro pueden ver y descargar acuerdos. Para obtener más información, consulteAdministrar un acuerdo para varias cuentas enAWSArtefactoen laAWS ArtifactGuía del usuario de.

Utilice la siguiente información como ayuda para integrar laAWS ArtifactporAWS Organizations.

Roles vinculados a servicios creados al habilitar la integración

Los siguientes ejemplos deRol vinculado al servicio deCuando habilita el acceso de confianza se crea automáticamente en la cuenta de administración de su organización. Este rol permiteAWS ArtifactPara realizar operaciones compatibles con las cuentas de su organización.

Puede eliminar o modificar esta función sólo si deshabilita el acceso de confianza entreAWS Artifacty Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSArtifactAccountSync`

Principales de servicio utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior sólo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Uso de roles vinculados a servicios deAWS Artifactconceder acceso a las siguientes entidades de servicio:

- `aws-artifact-account-sync.amazonaws.com`

Para habilitar el acceso de confianza conAWS Artifact

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consultePermisos necesarios para habilitar el acceso de confianza (p. 232).

Solo puede habilitar el acceso de confianza mediante las herramientas de Organizations.

Puede habilitar el acceso de confianza mediante laAWS Organizations, ejecutando unaAWS CLI, o llamando a una operación de API en uno de losAWSSDK de.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaServiciosEn la página, busque la fila deAWS Artifact, elija el nombre del servicio y, a continuación, elijaHabilitación del acceso de.
3. En el cuadro de diálogo de confirmación, habiliteMostrar la opción para habilitar el acceso de confianza, introduzca**`enable`**En el cuadro y, a continuación, elija.Habilitación del acceso de.
4. Si usted es el administrador de sóloAWS Organizations, dígale al administrador deAWS Artifactque ahora pueden habilitar ese servicio usando su consola para trabajar conAWS Organizations.

AWS CLI, AWS API

Para habilitar el acceso al servicio de confianza mediante Organizationscli/SDK

Puede utilizar las siguientes:AWS CLIPara habilitar el acceso del servicio de confianza:

- AWS CLI:enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitarAWS ArtifactServicio de confianza con Organizations de confianza.

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

Este comando no genera ninguna salida cuando se realiza correctamente.

- API de AWS: EnableAWSServiceAccess

Deshabilitación del acceso de confianza conAWS Artifact

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consultePermisos necesarios para deshabilitar el acceso de confianza (p. 233).

Sólo un administrador en elAWS OrganizationsPuede deshabilitar el acceso de confianza conAWS Artifact.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

AWS Artifactrequiere acceso de confianza conAWS Organizationspara trabajar con acuerdos de organización. Si deshabilita el acceso de confianza con AWS Organizations mientras utiliza AWS Artifact para trabajar con acuerdos de la organización, este deja de funcionar porque no puede obtener acceso a la organización. Todos los acuerdos de la organización que acepta en AWS Artifact se conservan, pero AWS Artifact no puede obtener acceso a ellos. La función de AWS Artifact que crea AWS Artifact se conserva. Si vuelve a habilitar el acceso de confianza, AWS Artifact seguirá funcionando como lo hacía antes sin necesidad de volver a configurar el servicio.

Una cuenta independiente que se elimine de una organización ya no tendrá acceso a ningún acuerdo de la organización.

Puede deshabilitar el acceso de confianza mediante laAWS Organizations, mediante la ejecución de una OrganizationsAWS CLI, o llamando a una operación de API de Organizations en uno de losAWSSDK de.

AWS Management Console

Para deshabilitar el acceso al servicio de confianza mediante la consola Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaServiciosEn la página, busque la fila deAWS Artifacty, a continuación, elija el nombre del servicio.
3. SeleccionarDeshabilitar el acceso de confianza.
4. En el cuadro de diálogo de confirmación, escriba**`disable`**En el cuadro y, a continuación, elija.Deshabilitar el acceso de confianza.
5. Si usted es el administrador de sóloAWS Organizations, dígale al administrador deAWS Artifactque ahora pueden deshabilitar ese servicio usando su consola o herramientas para trabajar conAWS Organizations.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante el CLI/SDK de Organizations

Puede utilizar las siguientes:AWS CLIPara deshabilitar el acceso del servicio de confianza:

- AWS CLI:disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitarAWS ArtifactServicio de confianza con Organizations de confianza.

```
$ aws organizations disable-aws-service-access \
    --service-principal aws-artifact-account-sync.amazonaws.com
```

Este comando no genera ninguna salida cuando se realiza correctamente.

- API de AWS: DisableAWSServiceAccess

AWS Audit Manager y AWS Organizations

AWS Audit Managerle ayuda a auditar continuamente suAWSPara simplificar la forma en que evalúa el riesgo y la conformidad con las normativas y los estándares del sector. Audit Manager automatiza la recopilación de evidencias para facilitar la evaluación de si sus políticas, procedimientos y actividades funcionan de manera eficaz. Cuando llega el momento de realizar una auditoría, el Audit Manager le ayuda a gestionar las revisiones de los controles de las partes interesadas y le ayuda a crear informes listos para auditorías con mucho menos esfuerzo manual.

Al integrar el Audit Manager conAWS Organizations, puede recopilar evidencia de una fuente más amplia incluyendo múltiples Cuentas de AWS En su organización dentro del alcance de sus evaluaciones.

Para obtener más información, consulteHabilitarAWSOrganizacionesen laGuía del usuario de Audit Manager.

Utilice la siguiente información como ayuda para integrar laAWS Audit ManagerporAWS Organizations.

Roles vinculados a servicios creados al habilitar la integración

Los siguientes ejemplos deRol vinculado al servicio deCuando habilita el acceso de confianza se crea automáticamente en la cuenta de administración de su organización. Esta función permite al Audit Manager realizar operaciones admitidas dentro de las cuentas de su organización.

Puede eliminar o modificar esta función sólo si deshabilita el acceso de confianza entre el Audit Manager y las Organizations, o si quita la cuenta de miembro de la organización.

Para obtener más información sobre cómo Audit Manager utiliza este rol, consulteUso de roles vinculados a serviciosen laAWS Audit ManagerGuía del usuario.

- `AWSServiceRoleForAuditManager`

Principales de servicio utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior sólo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Las funciones vinculadas a servicios utilizadas por Audit Manager otorgan acceso a las siguientes entidades de servicio:

- `auditmanager.amazonaws.com`

Para habilitar el acceso de confianza con el Audit Manager,

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consultePermisos necesarios para habilitar el acceso de confianza (p. 232).

El Audit Manager requiere un acceso de confianza aAWS OrganizationsAntes de designar una cuenta miembro para que sea el administrador delegado de su organización.

Puede habilitar el acceso de confianza mediante la consola de AWS Audit Manager o la consola de AWS Organizations.

> **Important**
>
> Le recomendamos que, en la medida de lo posible, utilice elAWS Audit Managero herramientas para habilitar la integración con Organizations. Esto le permiteAWS Audit Managerrealizar cualquier configuración que requiera, como la creación de los recursos necesarios para el servicio. Continúe con estos pasos solo si no puede habilitar la integración utilizando las herramientas proporcionadas porAWS Audit ManagerPara obtener más información, consulte.esta nota (p. 232).
> Si habilita el acceso de confianza mediante elAWS Audit ManagerConsola de la o las herramientas no necesita completar estos pasos.

Para habilitar el acceso de confianza mediante la consola Audit Manager

Para obtener instrucciones acerca de cómo habilitar el acceso de confianza, consulteConfiguraciónen laAWS Audit ManagerGuía del usuario de.

> **Note**
>
> Si configura un administrador delegado mediante laAWS Audit ManagerConsola de,AWS Audit Managerhabilita automáticamente el acceso de confianza para usted.

Puede habilitar el acceso de confianza ejecutando una OrganizationsAWS CLI, o llamando a una operación de API de Organizations en uno de losAWSSDK de.

AWS CLI, AWS API

Para habilitar el acceso a servicios de confianza mediante el CLI/SDK de Organizations

Puede utilizar las siguientes:AWS CLIPara habilitar el acceso del servicio de confianza:

- AWS CLI:enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitarAWS Audit ManagerServicio de confianza con Organizations de confianza.

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

  Este comando no genera ninguna salida cuando se realiza correctamente.
- API de AWS: EnableAWSServiceAccess

Para deshabilitar el acceso de confianza con el Audit Manager

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consultePermisos necesarios para deshabilitar el acceso de confianza (p. 233).

Sólo un administrador en elAWS OrganizationsPuede deshabilitar el acceso de confianza conAWS Audit Manager.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza ejecutando una OrganizationsAWS CLI, o llamando a una operación de API de Organizations en uno de losAWSSDK de.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante el CLI/SDK de Organizations

Puede utilizar las siguientes:AWS CLIPara deshabilitar el acceso del servicio de confianza:

- AWS CLI:disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitarAWS Audit ManagerServicio de confianza con Organizations de confianza.

```
$ aws organizations disable-aws-service-access \
    --service-principal auditmanager.amazonaws.com
```

  Este comando no genera ninguna salida cuando se realiza correctamente.
- API de AWS: DisableAWSServiceAccess

Para habilitar una cuenta de administrador delegado para Audit Manager

Cuando designa una cuenta de miembro como administrador delegado para la organización, los usuarios y los roles de esa cuenta pueden realizar acciones administrativas para el Audit Manager que, de lo contrario, sólo pueden realizar usuarios o roles en la cuenta de administración de la organización. Esto le ayuda a separar la administración de la organización de la gestión de Audit Manager.

Permisos mínimos

Sólo un usuario o rol de IAM en la cuenta de administración de Organizations con el siguiente permiso puede configurar una cuenta de miembro como administrador delegado para el Audit Manager de la organización:
`audit-manager:RegisterAccount`

Para obtener instrucciones acerca de cómo habilitar una cuenta de administrador delegada para el Audit Manager, consulteConfiguraciónen laAWS Audit ManagerGuía del usuario de.

Si configura un administrador delegado mediante laAWS Audit Managery, a continuación, el Audit Manager habilita automáticamente el acceso de confianza.

AWS CLI, AWS API

Si desea configurar una cuenta de administrador delegada mediante el comandoAWSCLI o uno de losAWSLos SDK, puede usar los siguientes comandos:

- AWS CLI:

```
$  aws audit-manager register-account \
    --delegated-admin-account 123456789012
```

- AWSSDK: Llame a`RegisterAccount`operar y proporcionar`delegatedAdminAccount`como parámetro para delegar la cuenta de administrador.

AWS Backup y AWS Organizations

AWS Backup es un servicio que le permite administrar y supervisar los trabajos de AWS Backup de su organización. Uso deAWS BackupSi inicia sesión como usuario en la cuenta de administración de la organización, puede habilitar la protección y supervisión de las copias de seguridad de toda la organización. Le ayuda a lograr la conformidad mediante el uso de políticas de copia de seguridad (p. 160) para aplicar planes de AWS Backup a los recursos de todas las cuentas de su organización de manera centralizada. Si usa AWS Backup y AWS Organizations juntos, puede obtener las siguientes ventajas:

Protección

Puede habilitar el tipo de política de copia de seguridad (p. 87) de su organización y, a continuación, crear políticas de copia de seguridad (p. 164) para asociarlas a la raíz, las unidades organizativas o las cuentas de la organización. Una política de copia de seguridad combina un plan de AWS Backup con el resto de detalles necesarios para aplicar el plan automáticamente a sus cuentas. Las políticas que están directamente asociadas a una cuenta se fusionan con las políticas heredadas (p. 97) de la raíz de la organización y de cualquier unidad organizativa principal para crear una política en vigor (p. 175) que se aplique a la cuenta. La directiva incluye el ID de un rol de IAM que tiene permisos para ejecutarAWS Backupen los recursos de sus cuentas.AWS Backuputiliza el rol de IAM para realizar la copia de seguridad en su nombre, tal como se especifica en el plan de copia de seguridad de la política en vigor.

Monitorización

Cuando habilita el acceso de confianza para AWS Backup (p. 234) en su organización, puede usar la consola de AWS Backup para ver detalles sobre los trabajos de copia de seguridad, restauración y copia de cualquiera de las cuentas de su organización. Para obtener más información, consulteMonitoree sus trabajos de backupen laAWS BackupGuía para desarrolladores.

Para obtener más información sobre AWS Backup, consulte la Guía para desarrolladores de AWS Backup.

Utilice la siguiente información como ayuda para integrar laAWS BackupporAWS Organizations.

Para habilitar el acceso de confianza conAWS Backup

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consultePermisos necesarios para habilitar el acceso de confianza (p. 232).

Puede habilitar el acceso de confianza mediante la consola de AWS Backup o la consola de AWS Organizations.

Important

Le recomendamos que, en la medida de lo posible, utilice elAWS Backupo herramientas para habilitar la integración con Organizations. Esto le permiteAWS Backuprealizar cualquier configuración que requiera, como la creación de los recursos necesarios para el servicio. Continúe con estos pasos solo si no puede habilitar la integración utilizando las herramientas proporcionadas porAWS BackupPara obtener más información, consulte.esta nota (p. 232). Si habilita el acceso de confianza mediante elAWS BackupConsola de la o las herramientas no necesita completar estos pasos.

Para habilitar el acceso de confianza medianteAWS Backup, consulteHabilitación de backup en varios Cuentas de AWS en laAWS BackupGuía para desarrolladores.

Deshabilitación del acceso de confianza conAWS Backup

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consultePermisos necesarios para habilitar el acceso de confianza (p. 232).

AWS Backuprequiere acceso de confianza conAWS OrganizationsPara habilitar la supervisión de los trabajos de copia de seguridad, restauración y copia en las cuentas de su organización. Si deshabilita el acceso de confianza con AWS Backup, pierde la capacidad de ver los trabajos que están fuera de la cuenta actual. La función de AWS Backup que crea AWS Backup se conserva. Si vuelve a habilitar el acceso de confianza, AWS Backup seguirá funcionando como lo hacía antes sin necesidad de volver a configurar el servicio.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza ejecutando una OrganizationsAWS CLI, o llamando a una operación de API de Organizations en uno de losAWSSDK de.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante el CLI/SDK de Organizations

Puede utilizar las siguientes:AWS CLIPara deshabilitar el acceso del servicio de confianza:

- AWS CLI:disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitarAWS BackupServicio de confianza con Organizations de confianza.

```
$ aws organizations disable-aws-service-access \
    --service-principal backup.amazonaws.com
```

  Este comando no genera ninguna salida cuando se realiza correctamente.
- API de AWS: DisableAWSServiceAccess

AWS CloudFormation StackSets y AWS Organizations

AWS CloudFormationStackSets permite crear, actualizar o eliminar pilas de varios Cuentas de AWS y Regiones de AWS con una sola operación. Integración de StackSets conAWS Organizationsle permite crear conjuntos de pilas con permisos administrados por servicios, utilizando un rol vinculado a servicios que tenga el permiso relevante en cada cuenta de miembro. Esto le permite implementar instancias de pila en cuentas miembro de la organización. No es preciso crear elAWS Identity and Access Management; StackSets crea el rol de IAM en cada cuenta de miembro en su nombre. También puede habilitar implementaciones automáticas en cuentas que se añaden a su organización en el futuro.

Con el acceso de confianza entre StackSets y Organizations habilitado, la cuenta de administración tiene permisos para crear y administrar conjuntos de pilas para su organización. La cuenta de administración puede registrar hasta cinco cuentas de miembros como administradores delegados. Con el acceso de confianza habilitado, los administradores delegados también tienen permisos para crear y administrar conjuntos de pilas para su organización. Los conjuntos de pila con permisos administrados por servicios se crean en la cuenta de gestión, incluidos los conjuntos de pila creados por administradores delegados.

> Important
>
> Los administradores delegados tienen permisos completos para implementar en cuentas de la organización. La cuenta de gestión no puede limitar los permisos del administrador delegado para implementar en unidades de organización específicas o para realizar operaciones específicas de conjuntos de pila.

Para obtener más información sobre la integración de StackSets con Organizations, consulteUso deAWSStackSets de CloudFormationen la AWS CloudFormation Guía del usuario de.

Utilice la siguiente información como ayuda para integrar laAWS CloudFormationStackSets conAWS Organizations.

Roles vinculados a servicios creados al habilitar la integración

Los siguientes ejemplos deRol vinculado al servicio deCuando habilita el acceso de confianza se crea automáticamente en la cuenta de administración de su organización. Este rol permiteAWS CloudFormationApilaciones para realizar operaciones admitidas dentro de las cuentas de su organización.

Puede eliminar o modificar esta función sólo si deshabilita el acceso de confianza entreAWS CloudFormationApilaciones y Organizations, o si quita la cuenta de miembro de la organización.

- Cuenta de administración:`CloudFormationStackSetsOrgAdmin`
- Cuentas de miembros`CloudFormationStackSetsOrgMember`

Principales de servicio utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior sólo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Uso de roles vinculados a servicios deAWS CloudFormationLos conjuntos de apilados otorgan acceso a las siguientes entidades de servicio:

- Cuenta de administración:`stacksets.cloudformation.amazonaws.com`

  Solo puede modificar o eliminar este rol si deshabilita el acceso de confianza entre StackSets y Organizations.
- Cuentas de miembros`member.org.stacksets.cloudformation.amazonaws.com`

  Solo puede modificar o eliminar este rol de una cuenta si deshabilita primero el acceso de confianza entre StackSets y Organizations, o si quita la cuenta primero de la organización o unidad organizativa (OU) de destino.

Para habilitar el acceso de confianza conAWS CloudFormationConjuntos de pilas de

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consultePermisos necesarios para habilitar el acceso de confianza (p. 232).

Solo un administrador de la cuenta de administración de Organizations tiene permisos para habilitar el acceso de confianza con otroAWSServicio Puede habilitar el acceso de confianza mediante la herramienta deAWS CloudFormationo la consola de Organizations.

Para habilitar el acceso de confianza a través deAWS CloudFormationStackSets.

Para habilitar el acceso de confianza mediante laAWS CloudFormationConsola de Stacksets, consulteHabilitación del acceso de confianza conAWS Organizationsen la AWS CloudFormation Guía del usuario de .

Deshabilitación del acceso de confianza conAWS CloudFormationConjuntos de pilas de

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consultePermisos necesarios para deshabilitar el acceso de confianza (p. 233).

Solo un administrador de una cuenta de administración de Organizations tiene permisos para deshabilitar el acceso de confianza con otroAWSServicio Sólo puede deshabilitar el acceso de confianza mediante la consola Organizations. Si deshabilita el acceso de confianza con Organizations mientras utiliza StackSets, se conservan todas las instancias de pila creadas previamente. Sin embargo, los conjuntos de pilas implementados con los permisos de la función vinculada a servicios ya no pueden realizar implementaciones en cuentas administradas por las Organizations.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza mediante laAWS Organizations, mediante la ejecución de una OrganizationsAWS CLI, o llamando a una operación de API de Organizations en uno de losAWSSDK de.

AWS Management Console

Para deshabilitar el acceso al servicio de confianza mediante la consola Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaServiciosEn la página, busque la fila deAWS CloudFormationConjuntos de pilasy, a continuación, elija el nombre del servicio.
3. SeleccionarDeshabilitar el acceso de confianza.
4. En el cuadro de diálogo de confirmación, escriba**`disable`**En el cuadro y, a continuación, elija.Deshabilitar el acceso de confianza.
5. Si usted es el administrador de sóloAWS Organizations, dígale al administrador deAWS CloudFormationStackSets ea que ahora pueden deshabilitar ese servicio usando su consola o herramientas para que no trabajen conAWS Organizations.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante el CLI/SDK de Organizations

Puede utilizar las siguientes:AWS CLIPara deshabilitar el acceso del servicio de confianza:

- AWS CLI:disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitarAWS CloudFormationStackSets como servicio de confianza con Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal stacksets.cloudformation.amazonaws.com
```

  Este comando no genera ninguna salida cuando se realiza correctamente.
- API de AWS: DisableAWSServiceAccess

Habilitación de una cuenta de administrador delegado paraAWS CloudFormationConjuntos de pilas de

Cuando designa una cuenta de miembro como administrador delegado para la organización, los usuarios y roles de esa cuenta pueden realizar acciones administrativas paraAWS CloudFormationApilaciones que, de lo contrario, sólo pueden realizar usuarios o roles en la cuenta de administración de la organización. Esto le ayuda a separar la gestión de la organización de la gestión deAWS CloudFormationStackSets

Para obtener instrucciones sobre cómo designar una cuenta de miembro como administrador delegado deAWS CloudFormationConjuntos de apilados en la organización, consulteRegistro de un administrador delegadoen laAWS CloudFormationGuía del usuario de.

AWS CloudTrail y AWS Organizations

AWS CloudTrailes unAWSque le ayuda a habilitar el gobierno, el cumplimiento, el funcionamiento y la auditoría de operaciones y riesgo de su Cuenta de AWS . Uso deAWS CloudTrail, un usuario de una cuenta de administración puede crear una pista de seguimiento de la organización que registre

todos los eventos de todos los Cuentas de AWS En esa organización. Los registros de seguimiento de la organización se aplican automáticamente a todas las cuentas de miembros de la organización. Las cuentas de miembros pueden ver el registro de seguimiento de la organización, pero no pueden modificarlo o eliminarlo. De forma predeterminada, las cuentas de miembros no tienen acceso a los archivos de registro del registro de seguimiento de la organización en el bucket de Amazon S3. Esto lo ayuda a aplicar y reforzar de manera uniforme su estrategia de registro entre las cuentas en su organización.

Para obtener más información, consulteCreación de un registro de seguimiento para una organizaciónen laAWS CloudTrailGuía del usuario de.

Utilice la siguiente información como ayuda para integrar laAWS CloudTrailporAWS Organizations.

Roles vinculados a servicios creados al habilitar la integración

Los siguientes ejemplos deRol vinculado al servicio deCuando habilita el acceso de confianza se crea automáticamente en la cuenta de administración de su organización. Esta función permite a CloudTrail realizar operaciones compatibles dentro de las cuentas de su organización.

Puede eliminar o modificar esta función sólo si deshabilita el acceso de confianza entre CloudTrail y Organizations, o si quita la cuenta de miembro de la organización.

- `AWSServiceRoleForCloudTrail`

Principales de servicio utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior sólo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios utilizados por CloudTrail otorgan acceso a las siguientes entidades de servicio:

- `cloudtrail.amazonaws.com`

Para habilitar el acceso de confianza con CloudTrail

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consultePermisos necesarios para habilitar el acceso de confianza (p. 232).

Puede habilitar el acceso de confianza mediante la consola de AWS CloudTrail o la consola de AWS Organizations.

> Important
>
> Le recomendamos que, en la medida de lo posible, utilice elAWS CloudTrailo herramientas para habilitar la integración con Organizations. Esto le permiteAWS CloudTrailrealizar cualquier configuración que requiera, como la creación de los recursos necesarios para el servicio. Continúe con estos pasos solo si no puede habilitar la integración utilizando las herramientas proporcionadas porAWS CloudTrailPara obtener más información, consulte.esta nota (p. 232). Si habilita el acceso de confianza mediante elAWS CloudTrailConsola de la o las herramientas no necesita completar estos pasos.

Debe iniciar sesión con suAWS OrganizationsPara crear una pista de seguimiento de organización. Si crea el registro de seguimiento desde la consola de AWS CloudTrail, el acceso de confianza se configura automáticamente. Si decide crear un registro de seguimiento de la organización mediante la AWS CLI o la API de AWS, debe configurar manualmente el acceso de confianza. Para obtener más información,

consulteHabilitar CloudTrail como servicio de confianza enAWS Organizationsen laAWS CloudTrailGuía del usuario de .

Puede habilitar el acceso de confianza ejecutando una OrganizationsAWS CLI, o llamando a una operación de API de Organizations en uno de losAWSSDK de.

AWS CLI, AWS API

Para habilitar el acceso a servicios de confianza mediante el CLI/SDK de Organizations

Puede utilizar las siguientes:AWS CLIPara habilitar el acceso del servicio de confianza:

- AWS CLI:enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitarAWS CloudTrailServicio de confianza con Organizations de confianza.

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

  Este comando no genera ninguna salida cuando se realiza correctamente.
- API de AWS: EnableAWSServiceAccess

Deshabilitación del acceso de confianza con CloudTrail

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consultePermisos necesarios para deshabilitar el acceso de confianza (p. 233).

AWS CloudTrailrequiere acceso de confianza conAWS Organizationspara trabajar con senderos de organización. Si deshabilitación del acceso de confianza medianteAWS Organizationsmientras utilizaAWS CloudTrailPara registros de seguimiento de la organización, los registros de seguimiento dejan de funcionar para las cuentas de miembros ya que CloudTrail no puede acceder a la organización. Los registros de seguimiento de la organización permanecen, igual que el`AWSServiceRoleForCloudTrail`creado para la integración entre CloudTrail yAWS Organizations. Si vuelve a habilitar el acceso de confianza, CloudTrail seguirá funcionando como lo hacía antes sin necesidad de volver a configurar los registros de seguimiento.

Sólo un administrador en elAWS OrganizationsPuede deshabilitar el acceso de confianza conAWS CloudTrail.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza mediante laAWS Organizations, mediante la ejecución de una OrganizationsAWS CLI, o llamando a una operación de API de Organizations en uno de losAWSSDK de.

AWS Management Console

Para deshabilitar el acceso al servicio de confianza mediante la consola Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaServiciosEn la página, busque la fila deAWS CloudTraily, a continuación, elija el nombre del servicio.
3. SeleccionarDeshabilitar el acceso de confianza.
4. En el cuadro de diálogo de confirmación, escriba**`disable`**En el cuadro y, a continuación, elija.Deshabilitar el acceso de confianza.

5. Si usted es el administrador de sóloAWS Organizations, dígale al administrador deAWS CloudTrailque ahora pueden deshabilitar ese servicio usando su consola o herramientas para trabajar conAWS Organizations.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante el CLI/SDK de Organizations

Puede utilizar las siguientes:AWS CLIPara deshabilitar el acceso del servicio de confianza:

- AWS CLI:disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitarAWS CloudTrailServicio de confianza con Organizations de confianza.

```
$ aws organizations disable-aws-service-access \
    --service-principal cloudtrail.amazonaws.com
```

  Este comando no genera ninguna salida cuando se realiza correctamente.
- API de AWS: DisableAWSServiceAccess

AWS Compute Optimizer y AWS Organizations

AWS Compute Optimizer es un servicio que analiza las métricas de configuración y utilización de sus recursos de AWS. Los ejemplos de recursos incluyen instancias de Amazon Elastic Compute Cloud (Amazon EC2) y grupos de Auto Scaling. Compute Optimizer informa de si sus recursos son óptimos y genera recomendaciones de optimización para reducir el costo y mejorar el desempeño de sus cargas de trabajo. Para obtener más información Compute Optimizer, consulte laAWS Compute OptimizerGuía del usuario de.

Utilice la siguiente información como ayuda para integrar laAWS Compute OptimizerporAWS Organizations.

Roles vinculados a servicios creados al habilitar la integración

Los siguientes ejemplos deRol vinculado al servicio deCuando habilita el acceso de confianza se crea automáticamente en la cuenta de administración de su organización. Esta función permite a Compute Optimizer realizar operaciones compatibles dentro de las cuentas de su organización.

Puede eliminar o modificar esta función sólo si deshabilita el acceso de confianza entre el Compute Optimizer y las Organizations, o si quita la cuenta de miembro de la organización.

- `AWSServiceRoleForComputeOptimizer`

Principales de servicio utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior sólo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios utilizados por Compute Optimizer otorgan acceso a las siguientes entidades de servicio:

- `compute-optimizer.amazonaws.com`

Habilitación del acceso de confianza Compute Optimizer de

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consultePermisos necesarios para habilitar el acceso de confianza (p. 232).

Puede habilitar el acceso de confianza mediante la consola de AWS Compute Optimizer o la consola de AWS Organizations.

> **Important**
>
> Le recomendamos que, en la medida de lo posible, utilice elAWS Compute Optimizero herramientas para habilitar la integración con Organizations. Esto le permiteAWS Compute Optimizerrealizar cualquier configuración que requiera, como la creación de los recursos necesarios para el servicio. Continúe con estos pasos solo si no puede habilitar la integración utilizando las herramientas proporcionadas porAWS Compute OptimizerPara obtener más información, consulte.esta nota (p. 232).
> Si habilita el acceso de confianza mediante elAWS Compute OptimizerConsola de la o las herramientas no necesita completar estos pasos.

Para habilitar el acceso de confianza mediante la consola de Compute Optimizer

Debe iniciar sesión en la consola de Compute Optimizer mediante la cuenta de administración de su organización. Suscríbete en nombre de tu organización siguiendo las instrucciones enDarse de baja en su cuentaen laAWS Compute OptimizerGuía del usuario de.

Puede habilitar el acceso de confianza mediante laAWS Organizations, ejecutando unaAWS CLI, o llamando a una operación de API en uno de losAWSSDK de.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaServiciosEn la página, busque la fila deAWS Compute Optimizer, elija el nombre del servicio y, a continuación, elijaHabilitación del acceso de.
3. En el cuadro de diálogo de confirmación, habiliteMostrar la opción para habilitar el acceso de confianza, introduzca**`enable`**En el cuadro y, a continuación, elija.Habilitación del acceso de.
4. Si usted es el administrador de sóloAWS Organizations, dígale al administrador deAWS Compute Optimizerque ahora pueden habilitar ese servicio usando su consola para trabajar conAWS Organizations.

AWS CLI, AWS API

Para habilitar el acceso al servicio de confianza mediante Organizationscli/SDK

Puede utilizar las siguientes:AWS CLIPara habilitar el acceso del servicio de confianza:

- AWS CLI:enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitarAWS Compute OptimizerServicio de confianza con Organizations de confianza.

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

  Este comando no genera ninguna salida cuando se realiza correctamente.

- API de AWS: EnableAWSServiceAccess

Deshabilitación del acceso de confianza con Compute Optimizer

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consultePermisos necesarios para deshabilitar el acceso de confianza (p. 233).

Sólo un administrador en elAWS OrganizationsPuede deshabilitar el acceso de confianza conAWS Compute Optimizer.

Puede deshabilitar el acceso de confianza ejecutando una OrganizationsAWS CLI, o llamando a una operación de API de Organizations en uno de losAWSSDK de.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante el CLI/SDK de Organizations

Puede utilizar las siguientes:AWS CLIPara deshabilitar el acceso del servicio de confianza:

- AWS CLI:disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitarAWS Compute OptimizerServicio de confianza con Organizations de confianza.

```
$ aws organizations disable-aws-service-access \
    --service-principal compute-optimizer.amazonaws.com
```

  Este comando no genera ninguna salida cuando se realiza correctamente.
- API de AWS: DisableAWSServiceAccess

AWS Config y AWS Organizations

Acumulación de datos de varias cuentas y regiones enAWS Configle permite agregarAWS Configy datos de varias cuentas Regiones de AWS en una sola cuenta. La acumulación de datos de varias cuentas y regiones permite a los administradores centrales de TI monitorear la conformidad de varias cuentas y regiones monitorear la Cuentas de AWS en la empresa. Un agregador es un tipo de recurso de AWS Config que recopila datos de AWS Config de varias cuentas y regiones de origen. Los agregadores se crean en la región en la que se desean ver los datos de AWS Config agregados. Al crear un agregador, puede seleccionar si desea añadir ID de cuenta individuales o su organización. Para obtener más información sobre AWS Config, consulte la AWS Config Guía para desarrolladores de .

También puede utilizarAWS ConfigAPI deAdministraciónAWS Configen todos los Cuentas de AWS En su organización, Para obtener más información, consulteHabilitaciónAWS ConfigReglas de en todas las cuentas de su organizaciónen la AWS Config Guía para desarrolladores.

Utilice la siguiente información como ayuda para integrar laAWS ConfigporAWS Organizations.

Roles vinculados a servicios creados al habilitar la integración

Los siguientes ejemplos deRol vinculado al servicio deSe crea en las cuentas de su organización cuando se habilita el acceso de confianza. Este rol permiteAWS ConfigPara realizar operaciones compatibles en las cuentas de su organización.

Este rol se crea cuando habilitaAWS Configen su organización mediante la creación de un agregador de varias cuentas.AWS Configle pide que seleccione o cree un rol y que proporcione el nombre. No hay un nombre generado automáticamente.

Puede eliminar o modificar esta función sólo si deshabilita el acceso de confianza entreAWS Configy Organizations, o si elimina la cuenta de miembro de la organización.

Para habilitar el acceso de confianza conAWS Config

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consultePermisos necesarios para habilitar el acceso de confianza (p. 232).

Puede habilitar el acceso de confianza mediante la consola de AWS Config o la consola de AWS Organizations.

> **Important**
>
> Le recomendamos que, en la medida de lo posible, utilice elAWS Configo herramientas para habilitar la integración con Organizations. Esto le permiteAWS Configrealizar cualquier configuración que requiera, como la creación de los recursos necesarios para el servicio. Continúe con estos pasos solo si no puede habilitar la integración utilizando las herramientas proporcionadas porAWS ConfigPara obtener más información, consulte.esta nota (p. 232). Si habilita el acceso de confianza mediante elAWS ConfigConsola de la o las herramientas no necesita completar estos pasos.

Para habilitar el acceso de confianza mediante laAWS Configconsole

Para habilitar el acceso de confianza aAWS OrganizationsconAWS ConfigPara crear un agregador de varias cuentas y agregar la organización. Para obtener información acerca de cómo configurar un agregador de varias cuentas, consulteConfiguración de un agregador mediante la consola deen la AWS Config Guía para desarrolladores.

Puede habilitar el acceso de confianza mediante laAWS Organizations, ejecutando unaAWS CLI, o llamando a una operación de API en uno de losAWSSDK de.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaServiciosEn la página, busque la fila deAWS Config, elija el nombre del servicio y, a continuación, elijaHabilitación del acceso de.
3. En el cuadro de diálogo de confirmación, habiliteMostrar la opción para habilitar el acceso de confianza, introduzca**`enable`**En el cuadro y, a continuación, elija.Habilitación del acceso de.
4. Si usted es el administrador de sóloAWS Organizations, dígale al administrador deAWS Configque ahora pueden habilitar ese servicio usando su consola para trabajar conAWS Organizations.

AWS CLI, AWS API

Para habilitar el acceso al servicio de confianza mediante Organizationscli/SDK

Puede utilizar las siguientes:AWS CLIPara habilitar el acceso del servicio de confianza:

- AWS CLI:enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitarAWS ConfigServicio de confianza con Organizations de confianza.

```
$ aws organizations enable-aws-service-access \
```

```
    --service-principal config.amazonaws.com
```

Este comando no genera ninguna salida cuando se realiza correctamente.

- API de AWS: EnableAWSServiceAccess

Deshabilitación del acceso de confianza conAWS Config

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consultePermisos necesarios para deshabilitar el acceso de confianza (p. 233).

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza ejecutando una OrganizationsAWS CLI, o llamando a una operación de API de Organizations en uno de losAWSSDK de.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante el CLI/SDK de Organizations

Puede utilizar las siguientes:AWS CLIPara deshabilitar el acceso del servicio de confianza:

- AWS CLI:disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitarAWS ConfigServicio de confianza con Organizations de confianza.

```
$ aws organizations disable-aws-service-access \
    --service-principal config.amazonaws.com
```

Este comando no genera ninguna salida cuando se realiza correctamente.

- API de AWS: DisableAWSServiceAccess

AWS Directory Service y AWS Organizations

AWS Directory Serviceo para Microsoft Active Directory,AWS Managed Microsoft AD, le permite ejecutar Microsoft Active Directory (AD) como un servicio administrado.AWS Directory Servicefacilita configurar y ejecutar directorios en laAWSNube o conecta tuAWSRecursos con un Microsoft Active Directory local existente.AWS Managed Microsoft ADtambién se integra estrechamente conAWS OrganizationsPara permitir el uso compartido sencillo de varios Cuentas de AWS y cualquier VPC en una región. Para obtener más información, consulte laAWS Directory ServiceGuía de administración.

Utilice la siguiente información como ayuda para integrarAWS Directory ServiceporAWS Organizations.

Para habilitar el acceso de confianza conAWS Directory Service

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consultePermisos necesarios para habilitar el acceso de confianza (p. 232).

Puede habilitar el acceso de confianza mediante la consola de AWS Directory Service o la consola de AWS Organizations.

Important

Le recomendamos que, en la medida de lo posible, utilice elAWS Directory Serviceo herramientas para habilitar la integración con Organizations. Esto le permiteAWS Directory Servicerealizar cualquier configuración que requiera, como la creación de los recursos necesarios para el

servicio. Continúe con estos pasos solo si no puede habilitar la integración utilizando las herramientas proporcionadas porAWS Directory ServicePara obtener más información, consulte.esta nota (p. 232).
Si habilita el acceso de confianza mediante elAWS Directory ServiceConsola de la o las herramientas no necesita completar estos pasos.

Para habilitar el acceso de confianza mediante laAWS Directory Serviceconsole

Para compartir un directorio, que habilita automáticamente el acceso de confianza, consulteCompartir el directorioen laAWS Directory ServiceGuía de administración. Para obtener instrucciones paso a paso, consulte.Tutorial: Compartir elAWSDirectorio administrado de Microsoft AD.

Puede habilitar el acceso de confianza mediante elAWS Organizationsconsola de .

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaServiciosEn la página, busque la fila deAWS Directory Service, elija el nombre del servicio y, a continuación, elijaHabilitación del acceso de.
3. En el cuadro de diálogo de confirmación, habiliteMostrar la opción para habilitar el acceso de confianza, introduzca**`enable`**En el cuadro y, a continuación, elija.Habilitación del acceso de.
4. Si usted es el administrador de sóloAWS Organizations, dígale al administrador deAWS Directory Serviceque ahora pueden habilitar ese servicio usando su consola para trabajar conAWS Organizations.

Deshabilitación del acceso de confianza conAWS Directory Service

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consultePermisos necesarios para deshabilitar el acceso de confianza (p. 233).

Si deshabilitación del acceso de confianza medianteAWS Organizationsmientras está usandoAWS Directory Service, todos los directorios compartidos anteriormente continúan funcionando de forma normal. Sin embargo, no puede compartir nuevos directorios en la organización hasta que habilite el acceso de confianza de nuevo.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza mediante elAWS Organizationsconsola de .

AWS Management Console

Para deshabilitar el acceso al servicio de confianza mediante la consola Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaServiciosEn la página, busque la fila deAWS Directory Servicey, a continuación, elija el nombre del servicio.
3. SeleccionarDeshabilitar el acceso de confianza.
4. En el cuadro de diálogo de confirmación, escriba**`disable`**En el cuadro y, a continuación, elija.Deshabilitar el acceso de confianza.

5. Si usted es el administrador de sóloAWS Organizations, dígale al administrador deAWS Directory Serviceque ahora pueden deshabilitar ese servicio usando su consola o herramientas para trabajar conAWS Organizations.

AWS Firewall Manager y AWS Organizations

AWS Firewall Manageres un servicio de administración de seguridad que utiliza para configurar y administrar de forma centralizada reglas de firewall y otras protecciones en toda la Cuentas de AWS Aplicaciones y aplicaciones de su organización. Con Firewall Manager, puede implementarAWS WAF, creeAWS Shield AdvancedConfigurar y auditar los grupos de seguridad de Amazon Virtual Private Cloud (Amazon VPC), e implementarAWS Network Firewall. Utilice Firewall Manager para configurar las protecciones una única vez de forma que se apliquen automáticamente en todas las cuentas y recursos de la organización, incluso cuando se añadan nuevas cuentas y recursos. Para obtener más información sobre AWS Firewall Manager, consulte la Guía para desarrolladores de AWS Firewall Manager.

Utilice la siguiente información como ayuda para integrarAWS Firewall ManagerporAWS Organizations.

Roles vinculados a servicios creados al habilitar la integración

Los siguientes ejemplos deRol vinculado al servicio deCuando habilita el acceso de confianza se crea automáticamente en la cuenta de administración de su organización. Esta función permite al Firewall Manager realizar operaciones compatibles en las cuentas de su organización.

Puede eliminar o modificar esta función sólo si deshabilita el acceso de confianza entre el Firewall Manager y las Organizations, o si quita la cuenta de miembro de la organización.

- `AWSServiceRoleForFMS`

Principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior sólo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios utilizados por Firewall Manager otorgan acceso a las siguientes entidades de servicio:

- `fms.amazonaws.com`

Habilitación del acceso de confianza Firewall Manager

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte.Permisos necesarios para habilitar el acceso de confianza (p. 232).

Puede habilitar el acceso de confianza mediante la consola de AWS Firewall Manager o la consola de AWS Organizations.

> **Important**
>
> Le recomendamos que, en la medida de lo posible, utilice elAWS Firewall Managero herramientas para habilitar la integración con Organizations. Esto le permiteAWS Firewall Managerrealizar cualquier configuración que requiera, como la creación de los recursos necesarios para el servicio. Continúe con estos pasos solo si no puede habilitar la integración utilizando las herramientas proporcionadas porAWS Firewall ManagerPara obtener más información, consulte.esta nota (p. 232).

Si habilita el acceso de confianza mediante elAWS Firewall ManagerConsola de la o las herramientas no necesita completar estos pasos.

Debe iniciar sesión con suAWS OrganizationsPara configurar una cuenta dentro de la organización como usuario de,AWS Firewall ManagerEn la cuenta de administrador. Para obtener más información, consulteEstablecimiento de la propiedad deAWS Firewall ManagerCuenta de administradoren laAWS Firewall ManagerGuía para desarrolladores.

Puede habilitar el acceso de confianza mediante laAWS Organizations, ejecutando unaAWS CLI, o llamando a una operación de API en uno de losAWSSDK de.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaServiciosEn la página, busque la fila deAWS Firewall Manager, elija el nombre del servicio y, a continuación, elijaHabilitación del acceso de.
3. En el cuadro de diálogo de confirmación, habiliteMostrar la opción para habilitar el acceso de confianza, introduzca**`enable`**En el cuadro y, a continuación, elija.Habilitación del acceso de.
4. Si usted es el administrador de sóloAWS Organizations, dígale al administrador deAWS Firewall Managerque ahora pueden habilitar ese servicio usando su consola para trabajar conAWS Organizations.

AWS CLI, AWS API

Para habilitar el acceso al servicio de confianza mediante Organizationscli/SDK

Puede utilizar las siguientes:AWS CLIPara habilitar el acceso del servicio de confianza:

- AWS CLI:enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitarAWS Firewall ManagerHabilitar como servicio de confianza con las Organizations.

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

  Este comando no genera ninguna salida cuando se realiza correctamente.
- API de AWS: EnableAWSServiceAccess

Deshabilitación del acceso de confianza con Firewall Manager

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consultePermisos necesarios para deshabilitar el acceso de confianza (p. 233).

Puede deshabilitar el acceso de confianza mediante la herramienta deAWS Firewall ManagerorAWS OrganizationsHerramientas.

Important

Le recomendamos que, en la medida de lo posible, utilice elAWS Firewall Managero herramientas para deshabilitar la integración con Organizations. Esto le permiteAWS Firewall Managerrealizar cualquier limpieza que requiera, como eliminar recursos o roles de acceso que ya no necesite

el servicio. Continúe con estos pasos solo si no puede deshabilitar la integración utilizando las herramientas proporcionadas porAWS Firewall Manager.
Si deshabilita el acceso de confianza mediante elAWS Firewall ManagerConsola de la o las herramientas no necesita completar estos pasos.

Para deshabilitar el acceso de confianza mediante la consola de Firewall Manager

Puede cambiar o revocar elAWS Firewall Managersiguiendo las instrucciones deDesignación de una cuenta diferente como cuenta deAWS Firewall ManagerCuenta de administradoren laAWS Firewall ManagerGuía para desarrolladores.

Si revoca la cuenta de administrador, debe iniciar sesión en laAWS Organizationsy establezca una nueva cuenta de administrador paraAWS Firewall Manager.

Puede deshabilitar el acceso de confianza mediante laAWS Organizations, mediante la ejecución de una OrganizationsAWS CLI, o llamando a una operación de API de Organizations en uno de losAWSSDK de.

AWS Management Console

Para deshabilitar el acceso al servicio de confianza mediante la consola Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaServiciosEn la página, busque la fila deAWS Firewall Managery, a continuación, elija el nombre del servicio.
3. SeleccionarDeshabilitar el acceso de confianza.
4. En el cuadro de diálogo de confirmación, escriba**`disable`**En el cuadro y, a continuación, elija.Deshabilitar el acceso de confianza.
5. Si usted es el administrador de sóloAWS Organizations, dígale al administrador deAWS Firewall Managerque ahora pueden deshabilitar ese servicio usando su consola o herramientas para trabajar conAWS Organizations.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante el CLI/SDK de Organizations

Puede utilizar las siguientes:AWS CLIPara deshabilitar el acceso del servicio de confianza:

- AWS CLI:disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitarAWS Firewall ManagerHabilitar como servicio de confianza con las Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal fms.amazonaws.com
```

  Este comando no genera ninguna salida cuando se realiza correctamente.
- API de AWS: DisableAWSServiceAccess

Para habilitar una cuenta de administrador delegado para Firewall Manager

Cuando designa una cuenta de miembro como administrador delegado para la organización, los usuarios y las funciones de esa cuenta pueden realizar acciones administrativas para Firewall Manager que,

de lo contrario, sólo pueden ser realizadas por usuarios o roles en la cuenta de administración de la organización. Esto le ayuda a separar la administración de la organización de la administración de Firewall Manager.

Permisos mínimos

Sólo un usuario o rol de IAM en la cuenta de administración de Organizations puede configurar una cuenta de miembro como administrador delegado para Firewall Manager en la organización.

Para obtener instrucciones acerca de cómo designar una cuenta de miembro como administrador de Firewall Manager para la organización, consulteEstablecimiento de la propiedad deAWS Firewall ManagerCuenta de administradoren laAWS Firewall ManagerGuía para desarrolladores.

Amazon GuardDuty yAWS Organizations

Amazon GuardDuty es un servicio de monitorización continua de la seguridad que analiza y procesa una variedad de fuentes de datos, utilizando fuentes de información de amenazas y aprendizaje automático para identificar la actividad inesperada y potencialmente no permitida, así como la actividad malintencionada en suAWSMedio ambiente. Esto puede incluir problemas como escalado de privilegios, uso de credenciales expuestas o la comunicación con direcciones IP, URL o dominios malintencionados.

Puede ayudar a simplificar la administración de GuardDuty mediante el uso de Organizations para administrar GuardDuty en todas las cuentas de su organización.

Para obtener más información, consulteAdministrar cuentas de GuardDuty conAWS Organizationsen laGuía del usuario de Amazon GuardDuty

Utilice la siguiente información como ayuda para integrar Amazon GuardDuty conAWS Organizations.

Roles vinculados a servicios creados al habilitar la integración

Los siguientes ejemplos deRol vinculado al servicio deCuando habilita el acceso de confianza se crea automáticamente en la cuenta de administración de su organización. Esta función permite a GuardDuty realizar operaciones compatibles dentro de las cuentas de su organización.

Puede eliminar o modificar este rol sólo si deshabilita el acceso de confianza entre GuardDuty y Organizations, o si quita la cuenta de miembro de la organización.

- `AWSServiceRoleForAmazonGuardDuty`

Principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior sólo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios utilizados por GuardDuty otorgan acceso a las siguientes entidades de servicio:

- `guardduty.amazonaws.com`

Peritación del acceso de confianza con GuardDuty

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte.Permisos necesarios para habilitar el acceso de confianza (p. 232).

Puede habilitar el acceso de confianza mediante Amazon GuardDuty.

Amazon GuardDuty requiere un acceso de confianza aAWS OrganizationsAntes de designar una cuenta miembro para que sea el administrador de GuardDuty de su organización. Si configura un administrador delegado mediante la consola de GuardDuty, GuardDuty habilita automáticamente el acceso de confianza.

Sin embargo, si desea configurar una cuenta de administrador delegada mediante elAWS CLIo uno de losAWSSDK, debe llamar de forma explícita aEnableAWSServiceAccessy proporcionar la entidad de servicio como parámetro. Entonces puede llamarEnableOrganizationAdminAccountpara delegar la cuenta de administrador de GuardDuty.

Deshabilitación del acceso de confianza con GuardDuty

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consultePermisos necesarios para deshabilitar el acceso de confianza (p. 233).

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza ejecutando una OrganizationsAWS CLI, o llamando a una operación de API de Organizations en uno de losAWSSDK de.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante el CLI/SDK de Organizations

Puede utilizar las siguientes:AWS CLIPara deshabilitar el acceso del servicio de confianza:

- AWS CLI:disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitar Amazon GuardDuty como servicio de confianza con Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal guardduty.amazonaws.com
```

  Este comando no genera ninguna salida cuando se realiza correctamente.
- API de AWS: DisableAWSServiceAccess

Habilitación de una cuenta de administrador delegado para GuardDuty

Cuando designa una cuenta de miembro como administrador delegado para la organización, los usuarios y roles de esa cuenta pueden realizar acciones administrativas para GuardDuty que, de lo contrario, sólo pueden ser realizadas por usuarios o roles en la cuenta de administración de la organización. Esto le ayuda a separar la gestión de la organización de la gestión de GuardDuty.

Permisos mínimos

Para obtener información acerca de los permisos necesarios para designar una cuenta de miembro como administrador delegado, consultePermisos necesarios para designar un administrador delegadoen laGuía del usuario de Amazon GuardDuty

Para designar una cuenta de miembro como administrador delegado para GuardDuty

ConsulteDesigne un administrador delegado y agregue cuentas miembro (consola)yDesigne un administrador delegado y agregue cuentas miembro (API)

AWS Health y AWS Organizations

AWS Healthproporciona una visibilidad continua del rendimiento de sus recursos y la disponibilidad de suAWSservicios y cuentas.AWS Healthofrece eventos cuando suAWSrecursos y servicios se ven afectados por un problema o se verán afectados por los próximos cambios. Después de habilitar la vista organizativa, un usuario de la cuenta de administración de la organización puede agregarAWS HealthEventos en todas las cuentas de la organización. Solo muestra la vista organizativa.AWS Healthentregados después de que la función esté habilitada y los retiene durante 90 días.

Puede habilitar la vista organizativa mediante la herramienta deAWS HealthConsola de, elAWS Command Line Interface(AWS CLI), o elAWS HealthAPI.

Para obtener más información, consulteAggregateAWS HealthEventos deen laAWS HealthGuía del usuario de.

Utilice la siguiente información como ayuda para integrarAWS HealthporAWS Organizations.

Roles vinculados a servicios creados al habilitar la integración

Los siguientes ejemplos deRol vinculado al servicio deCuando habilita el acceso de confianza se crea automáticamente en la cuenta de administración de su organización. Este rol permiteAWS HealthPara realizar operaciones compatibles con las cuentas de su organización.

Puede eliminar o modificar esta función sólo si deshabilita el acceso de confianza entreAWS Healthy Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForHealth_Organizations`

Principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior sólo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Uso de roles vinculados a servicios deAWS Healthconceder acceso a las siguientes entidades de servicio:

- `health.amazonaws.com`

Para habilitar el acceso de confianza conAWS Health

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte.Permisos necesarios para habilitar el acceso de confianza (p. 232).

Cuando se habilita la función de vista organizativa paraAWS Health, el acceso de confianza también se habilita automáticamente.

Puede habilitar el acceso de confianza mediante la consola de AWS Health o la consola de AWS Organizations.

> **Important**
>
> Le recomendamos que, en la medida de lo posible, utilice elAWS Healtho herramientas para habilitar la integración con Organizations. Esto le permiteAWS Healthrealizar cualquier configuración que requiera, como la creación de los recursos necesarios para el servicio.

Continúe con estos pasos solo si no puede habilitar la integración utilizando las herramientas proporcionadas porAWS HealthPara obtener más información, consulte.esta nota (p. 232).
Si habilita el acceso de confianza mediante elAWS HealthConsola de la o las herramientas no necesita completar estos pasos.

Para habilitar el acceso de confianza mediante laAWS Healthconsole

Puede deshabilitar el acceso de confianza mediante una de las siguientes opciones:

Puede habilitar el acceso de confianza utilizandoAWS Healthy una de las siguientes opciones:

- Use la consola de AWS Health. Para obtener más información, consulteVista organizativa (consola)en laAWS HealthGuía del usuario de.
- Use la AWS CLI. Para obtener más información, consulteVista organizativa (CLI)en laAWS HealthGuía del usuario de.
- Llame aEnableHealthServiceAccessForOrganizationOperación de la API.

Puede habilitar el acceso de confianza ejecutando una OrganizationsAWS CLI, o llamando a una operación de API de Organizations en uno de losAWSSDK de.

AWS CLI, AWS API

Para habilitar el acceso a servicios de confianza mediante el CLI/SDK de Organizations

Puede utilizar las siguientes:AWS CLIPara habilitar el acceso del servicio de confianza:

- AWS CLI:enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitarAWS HealthHabilitar como servicio de confianza con las Organizations.

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

  Este comando no genera ninguna salida cuando se realiza correctamente.
- API de AWS: EnableAWSServiceAccess

Deshabilitación del acceso de confianza conAWS Health

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consultePermisos necesarios para deshabilitar el acceso de confianza (p. 233).

Después de deshabilitar la función de vista organizativa,AWS HealthDetiene la agregación de eventos para todas las demás cuentas de su organización. Esto también deshabilita automáticamente el acceso de confianza.

Puede deshabilitar el acceso de confianza mediante la herramienta deAWS HealthorAWS OrganizationsHerramientas.

Important

Le recomendamos que, en la medida de lo posible, utilice elAWS Healtho herramientas para deshabilitar la integración con Organizations. Esto le permiteAWS Healthrealizar cualquier limpieza que requiera, como eliminar recursos o roles de acceso que ya no necesite el servicio. Continúe con estos pasos solo si no puede deshabilitar la integración utilizando las herramientas proporcionadas porAWS Health.

Si deshabilita el acceso de confianza mediante elAWS HealthConsola de la o las herramientas no necesita completar estos pasos.

Para deshabilitar el acceso de confianza mediante laAWS Healthconsole

Puede deshabilitar el acceso de confianza mediante una de las siguientes opciones:

- Use la consola de AWS Health. Para obtener más información, consulteDeshabilitación de la vista organizativa (consola)en laAWS HealthGuía del usuario de.
- Use la AWS CLI. Para obtener más información, consulteDeshabilitación de la vista organizativa (CLI)en laAWS HealthGuía del usuario de.
- Llame aDisableHealthServiceAccessForOrganizationOperación de la API.

Puede deshabilitar el acceso de confianza ejecutando una OrganizationsAWS CLI, o llamando a una operación de API de Organizations en uno de losAWSSDK de.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante el CLI/SDK de Organizations

Puede utilizar las siguientes:AWS CLIPara deshabilitar el acceso del servicio de confianza:

- AWS CLI:disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitarAWS HealthHabilitar como servicio de confianza con las Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal health.amazonaws.com
```

  Este comando no genera ninguna salida cuando se realiza correctamente.
- API de AWS: DisableAWSServiceAccess

AWS License Manager y AWS Organizations

AWS License Manager simplifica el proceso de llevar licencias de proveedores de software a la nube. A medida que construye la infraestructura en la nube enAWSCon, puede ahorrar en costos mediante el uso de oportunidades «Bring-Your-Own-License (BYOL)», es decir, reconvirtiendo su inventario de licencias para utilizarlo con los recursos de la nube. Con controles basados en reglas en el consumo de licencias, los administradores pueden establecer límites fijos o flexibles en las implementaciones nuevas o existentes en la nube, impidiendo de este modo el uso de servidor no conforme antes de que se produzca.

Al vincular License Manager conAWS OrganizationsPuede habilitar el descubrimiento entre cuentas de recursos informáticos en toda su organización.

Para obtener más información acerca del License Manager de, consulte laLicense Manager: License Manager.

Utilice la siguiente información como ayuda para integrarAWS License ManagerporAWS Organizations.

Roles vinculados a servicios creados al habilitar la integración

Los siguientes ejemplos deRol vinculado al servicio deCuando habilita el acceso de confianza se crea automáticamente en la cuenta de administración de su organización. Esta función permite al License Manager realizar operaciones compatibles dentro de las cuentas de su organización.

Puede eliminar o modificar esta función sólo si deshabilita el acceso de confianza entre License Manager y Organizations, o si quita la cuenta de miembro de la organización.

- `AWSLicenseManagerMasterAccountRole`
- `AWSLicenseManagerMemberAccountRole`
- `AWSServiceRoleForAWSLicenseManagerRole`

Para obtener más información, consulteUso de la función de cuenta Administrador de licencias: administraciónyUso de la función Administrador de licencias: cuenta de miembro.

Principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior sólo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios utilizados por License Manager otorgan acceso a las siguientes entidades de servicio:

- `license-manager.amazonaws.com`
- `license-manager.member-account.amazonaws.com`

Habilitación del acceso de confianza con License Manager

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte.Permisos necesarios para habilitar el acceso de confianza (p. 232).

Puede habilitar el acceso de confianza medianteAWS License Manager.

Para habilitar el acceso de confianza con License Manager

Debe iniciar sesión en la consola de License Manager con suAWS Organizationsy asóciela a su cuenta de License Manager. Para obtener más información, consulteConfiguraciónAWS License ManagerConfiguración de la guía. También se resume aquí para mayor comodidad.

> **Important**
>
> Este procedimiento es una puerta unidireccional. No podrá deshacer esto.

Para habilitar el acceso de confianza entre Organizations y License Manager

1. Inicie sesión enAWS Management Consoleutilizando la cuenta de administración de su organización.
2. Vaya a la .Consola de License Managery elijaConfiguración.
3. Elija Edit (Editar).
4. SeleccionarEnlaceAWS Organizationscuentas.

Deshabilitación del acceso de confianza con License Manager

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consultePermisos necesarios para deshabilitar el acceso de confianza (p. 233).

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza ejecutando una OrganizationsAWS CLI, o llamando a una operación de API de Organizations en uno de losAWSSDK de.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante el CLI/SDK de Organizations

Puede utilizar las siguientes:AWS CLIPara deshabilitar el acceso del servicio de confianza:

- AWS CLI:disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitarAWS License ManagerHabilitar como servicio de confianza con las Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal license-manager.amazonaws.com
```

  Este comando no genera ninguna salida cuando se realiza correctamente.
- API de AWS: DisableAWSServiceAccess

Para habilitar una cuenta de administrador delegado para License Manager

Cuando designa una cuenta de miembro como administrador delegado para la organización, los usuarios y las funciones de esa cuenta pueden realizar acciones administrativas para License Manager que, de lo contrario, sólo pueden ser realizadas por usuarios o roles en la cuenta de administración de la organización. Esto le ayuda a separar la administración de la organización de la administración de License Manager.

Para delegar una cuenta de miembro como administrador para License Manager, siga los pasos que se indican enRegistro de un administrador delegadoen laLicense Manager: License Manager. También se resumen aquí para su conveniencia.

Para registrar una cuenta de administrador delegado para License Manager

1. Inicie sesión enAWS Management Consoleutilizando la cuenta de administración de su organización.
2. Vaya a la .Consola de License Managery elijaConfiguración.
3. UNDERAdministrador delegado, elijaAdministrador delegado.
4. Introduzca el número de ID de cuenta para el Cuenta de AWS Seleccione y, a continuación, elijaDelegate. No puedes usar el ID para la cuenta de administración. Debe ser una cuenta de miembro.

Amazon Macie yAWS Organizations

Amazon Macie es un servicio de privacidad y seguridad de datos totalmente gestionado que utiliza aprendizaje automático y coincidencia de patrones para descubrir, supervisar y ayudar a proteger sus datos confidenciales en Amazon Simple Storage Service (Amazon S3). Macie automatiza el descubrimiento de datos confidenciales, como información de identificación personal (PII) y propiedad intelectual, para proporcionarle una mejor comprensión de los datos que almacena su organización en Amazon S3.

Para obtener más información, consulteGestionar varias cuentas de Amazon Macie conAWS Organizationsen laGuía del usuario de Amazon Macie.

Utilice la siguiente información como ayuda para integrar Amazon Macie conAWS Organizations.

Roles vinculados a servicios creados al habilitar la integración

Los siguientes ejemplos deRol vinculado al servicio deCuando habilita el acceso de confianza se crea automáticamente en la cuenta de administración de su organización. Este rol permite a Macie realizar operaciones admitidas dentro de las cuentas de su organización.

Puede eliminar o modificar este rol sólo si deshabilita el acceso de confianza entre Macie y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleRorAmazonMacie`

Principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior sólo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios utilizados por Macie otorgan acceso a las siguientes entidades de servicio:

- `macie.amazonaws.com`

Para habilitar el acceso de confianza con Macie

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte.Permisos necesarios para habilitar el acceso de confianza (p. 232).

Puede habilitar el acceso de confianza mediante la consola de Amazon Macie o laAWS Organizationsconsola de .

> Important
>
> Le recomendamos encarecidamente que, siempre que sea posible, utilice la consola o las herramientas de Amazon Macie para habilitar la integración con las Organizations. Esto permite a Amazon Macie realizar cualquier configuración que requiera, como la creación de los recursos necesarios para el servicio. Siga estos pasos solo si no puede habilitar la integración mediante las herramientas proporcionadas por Amazon Macie.Para obtener más información, consulteesta nota (p. 232).
> Si habilitas el acceso de confianza mediante la consola o las herramientas de Amazon Macie, no tendrás que completar estos pasos.

Para habilitar el acceso de confianza mediante la consola de Macie consola de

Amazon Macie requiere acceso de confianza aAWS OrganizationsPara designar una cuenta de miembro para que sea administrador de Macie de su organización. Si configura un administrador delegado mediante la consola de administración de Macie, Macie habilita automáticamente el acceso de confianza.

Para obtener más información, consulteHabilitación del acceso de confianza conAWS Organizationsen laGuía del usuario de Amazon Macie.

Puede habilitar el acceso de confianza ejecutando una OrganizationsAWS CLI, o llamando a una operación de API de Organizations en uno de losAWSSDK de.

AWS CLI, AWS API

> Para habilitar el acceso a servicios de confianza mediante el CLI/SDK de Organizations
>
> Puede utilizar las siguientes:AWS CLIPara habilitar el acceso del servicio de confianza:

- AWS CLI:enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitar Amazon Macie como servicio de confianza con Organizations.

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

  Este comando no genera ninguna salida cuando se realiza correctamente.
- API de AWS: EnableAWSServiceAccess

Habilitación de una cuenta de administrador delegado para Macie

Cuando designa una cuenta de miembro como administrador delegado para la organización, los usuarios y roles de esa cuenta pueden realizar acciones administrativas para Macie que, de lo contrario, sólo pueden ser realizadas por usuarios o roles en la cuenta de administración de la organización. Esto le ayuda a separar la gestión de la organización de la gestión de Macie.

Permisos mínimos

Sólo un usuario o rol de IAM en la cuenta de administración de Organizations con los siguientes permisos puede configurar una cuenta de miembro como administrador delegado para Macie en la organización:

- `organizations:EnableAWSServiceAccess`
- `macie:EnableOrganizationAdminAccount`

Para designar una cuenta de miembro como administrador delegado para Macie

Amazon Macie requiere acceso de confianza aAWS OrganizationsPara designar una cuenta de miembro para que sea administrador de Macie de su organización. Si configura un administrador delegado mediante la consola de administración de Macie, Macie habilita automáticamente el acceso de confianza.

Para obtener más información, consultehttps://docs.aws.amazon.com/macie/latest/user/macie-organizations.html#register-delegated-admin

AWS Marketplace y AWS Organizations

AWS Marketplace es un catálogo digital seleccionado que puede utilizar para buscar, comprar, implementar y administrar software, datos y servicios de terceros que necesita para desarrollar soluciones y hacer funcionar sus negocios.

AWS Marketplace crea y administra licencias medianteAWS License Managerpara tus compras en AWS Marketplace . Cuando comparta (concede acceso a) sus licencias con otras cuentas de su organización, AWS Marketplace crea y administra nuevas licencias para esas cuentas.

Para obtener más información, consulteRoles vinculados a servicios de AWS Marketplace en la AWS Marketplace Guía del comprador de.

Utilice la siguiente información como ayuda para integrar AWS Marketplace porAWS Organizations.

Roles vinculados a servicios creados al habilitar la integración

Los siguientes ejemplos deRol vinculado al servicio deCuando habilita el acceso de confianza se crea automáticamente en la cuenta de administración de su organización. Este rol permite AWS Marketplace Para realizar operaciones compatibles con las cuentas de su organización.

Puede eliminar o modificar esta función sólo si deshabilita el acceso de confianza entre AWS Marketplace y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForMarketplaceLicenseManagement`

Principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior sólo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Uso de roles vinculados a servicios de AWS Marketplace conceder acceso a las siguientes entidades de servicio:

- `license-management.marketplace.amazonaws.com`

Para habilitar el acceso de confianza con AWS Marketplace

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte.Permisos necesarios para habilitar el acceso de confianza (p. 232).

Puede habilitar el acceso de confianza mediante la consola de AWS Marketplace o la consola de AWS Organizations.

> Important
>
> Le recomendamos que, en la medida de lo posible, utilice el AWS Marketplace o herramientas para habilitar la integración con Organizations. Esto le permite AWS Marketplace realizar cualquier configuración que requiera, como la creación de los recursos necesarios para el servicio. Continúe con estos pasos solo si no puede habilitar la integración utilizando las herramientas proporcionadas por AWS Marketplace Para obtener más información, consulte.esta nota (p. 232).
> Si habilita el acceso de confianza mediante el AWS Marketplace Consola de la o las herramientas no necesita completar estos pasos.

Para habilitar el acceso de confianza mediante la AWS Marketplace console

consulteCreación de un rol vinculado a un servicio de AWS Marketplace en la AWS Marketplace Guía del comprador de.

Puede habilitar el acceso de confianza mediante laAWS Organizations, ejecutando unaAWS CLI, o llamando a una operación de API en uno de losAWSSDK de.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaServiciosEn la página, busque la fila de AWS Marketplace , elija el nombre del servicio y, a continuación, elijaHabilitación del acceso de.
3. En el cuadro de diálogo de confirmación, habiliteMostrar la opción para habilitar el acceso de confianza, introduzca**`enable`**En el cuadro y, a continuación, elija.Habilitación del acceso de.
4. Si usted es el administrador de sóloAWS Organizations, dígale al administrador de AWS Marketplace que ahora pueden habilitar ese servicio usando su consola para trabajar conAWS Organizations.

AWS CLI, AWS API

Para habilitar el acceso al servicio de confianza mediante Organizationscli/SDK

Puede utilizar las siguientes:AWS CLIPara habilitar el acceso del servicio de confianza:

- AWS CLI:enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitar AWS Marketplace Habilitar como servicio de confianza con las Organizations.

```
$ aws organizations enable-aws-service-access \
    --service-principal license-management.marketplace.amazonaws.com
```

  Este comando no genera ninguna salida cuando se realiza correctamente.
- API de AWS: EnableAWSServiceAccess

Deshabilitación del acceso de confianza con AWS Marketplace

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte.Permisos necesarios para habilitar el acceso de confianza (p. 232).

Solo puede habilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza ejecutando una OrganizationsAWS CLI, o llamando a una operación de API de Organizations en uno de losAWSSDK de.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante el CLI/SDK de Organizations

Puede utilizar las siguientes:AWS CLIPara deshabilitar el acceso del servicio de confianza:

- AWS CLI:disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitar AWS Marketplace Habilitar como servicio de confianza con las Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal license-management.marketplace.amazonaws.com
```

  Este comando no genera ninguna salida cuando se realiza correctamente.
- API de AWS: DisableAWSServiceAccess

AWS Resource Access Manager y AWS Organizations

AWS Resource Access Manager(AWS RAM) le permite compartirAWSUso de recursos de su propiedad con otros Cuentas de AWS . Es un servicio centralizado que proporciona una experiencia coherente para compartir distintos tipos de recursos de AWS en varias cuentas.

Para obtener más información acerca de AWS RAM, consulte la Guía del usuario de AWS RAM.

Utilice la siguiente información como ayuda para integrarAWS Resource Access ManagerporAWS Organizations.

Roles vinculados a servicios creados al habilitar la integración

Los siguientes ejemplos deRol vinculado al servicio deCuando habilita el acceso de confianza se crea automáticamente en la cuenta de administración de su organización. Este rol permiteAWS RAMPara realizar operaciones compatibles con las cuentas de su organización.

Puede eliminar o modificar esta función sólo si deshabilita el acceso de confianza entreAWS RAMy Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForResourceAccessManager`

Principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior sólo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Uso de roles vinculados a servicios deAWS RAMconceder acceso a las siguientes entidades de servicio:

- `ram.amazonaws.com`

Para habilitar el acceso de confianza conAWS RAM

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte.Permisos necesarios para habilitar el acceso de confianza (p. 232).

Puede habilitar el acceso de confianza mediante la consola de AWS Resource Access Manager o la consola de AWS Organizations.

> **Important**
>
> Le recomendamos que, en la medida de lo posible, utilice elAWS Resource Access Managero herramientas para habilitar la integración con Organizations. Esto le permiteAWS Resource Access Managerrealizar cualquier configuración que requiera, como la creación de los recursos necesarios para el servicio. Continúe con estos pasos solo si no puede habilitar la integración utilizando las herramientas proporcionadas porAWS Resource Access ManagerPara obtener más información, consulte.esta nota (p. 232).
> Si habilita el acceso de confianza mediante elAWS Resource Access ManagerConsola de la o las herramientas no necesita completar estos pasos.

Para habilitar el acceso de confianza a través de laAWS RAMConsola o CLI

ConsulteHabilitar el uso compartido conAWS Organizationsen laAWS RAMGuía del usuario de.

Puede habilitar el acceso de confianza mediante laAWS Organizations, ejecutando unaAWS CLI, o llamando a una operación de API en uno de losAWSSDK de.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaServiciosEn la página, busque la fila deAWS Resource Access Manager, elija el nombre del servicio y, a continuación, elijaHabilitación del acceso de.

3. En el cuadro de diálogo de confirmación, habiliteMostrar la opción para habilitar el acceso de confianza, introduzca**`enable`**En el cuadro y, a continuación, elija.Habilitación del acceso de.
4. Si usted es el administrador de sóloAWS Organizations, dígale al administrador deAWS Resource Access Managerque ahora pueden habilitar ese servicio usando su consola para trabajar conAWS Organizations.

AWS CLI, AWS API

Para habilitar el acceso al servicio de confianza mediante Organizationscli/SDK

Puede utilizar las siguientes:AWS CLIPara habilitar el acceso del servicio de confianza:

- AWS CLI:enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitarAWS Resource Access ManagerHabilitar como servicio de confianza con las Organizations.

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

  Este comando no genera ninguna salida cuando se realiza correctamente.
- API de AWS: EnableAWSServiceAccess

Deshabilitación del acceso de confianza conAWS RAM

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consultePermisos necesarios para deshabilitar el acceso de confianza (p. 233).

Puede deshabilitar el acceso de confianza mediante la herramienta deAWS Resource Access ManagerorAWS OrganizationsHerramientas.

> **Important**
>
> Le recomendamos que, en la medida de lo posible, utilice elAWS Resource Access Managero herramientas para deshabilitar la integración con Organizations. Esto le permiteAWS Resource Access Managerrealizar cualquier limpieza que requiera, como eliminar recursos o roles de acceso que ya no necesite el servicio. Continúe con estos pasos solo si no puede deshabilitar la integración utilizando las herramientas proporcionadas porAWS Resource Access Manager.
> Si deshabilita el acceso de confianza mediante elAWS Resource Access ManagerConsola de la o las herramientas no necesita completar estos pasos.

Para habilitar el acceso de confianza a través de laAWS Resource Access ManagerConsola o CLI

ConsulteHabilitar el uso compartido conAWS Organizationsen laAWS RAMGuía del usuario de.

Puede deshabilitar el acceso de confianza mediante laAWS Organizations, mediante la ejecución de una OrganizationsAWS CLI, o llamando a una operación de API de Organizations en uno de losAWSSDK de.

AWS Management Console

Para deshabilitar el acceso al servicio de confianza mediante la consola Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.

2. En la páginaServiciosEn la página, busque la fila deAWS Resource Access Managery, a continuación, elija el nombre del servicio.
3. SeleccionarDeshabilitar el acceso de confianza.
4. En el cuadro de diálogo de confirmación, escriba**`disable`**En el cuadro y, a continuación, elija.Deshabilitar el acceso de confianza.
5. Si usted es el administrador de sóloAWS Organizations, dígale al administrador deAWS Resource Access Managerque ahora pueden deshabilitar ese servicio usando su consola o herramientas para trabajar conAWS Organizations.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante el CLI/SDK de Organizations

Puede utilizar las siguientes:AWS CLIPara deshabilitar el acceso del servicio de confianza:

- AWS CLI:disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitarAWS Resource Access ManagerHabilitar como servicio de confianza con las Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal ram.amazonaws.com
```

  Este comando no genera ninguna salida cuando se realiza correctamente.
- API de AWS: DisableAWSServiceAccess

AWS Security Hub y AWS Organizations

AWS Security Hub le proporciona una visión completa de su estado de seguridad en AWS y le ayuda a comprobar su entorno con los estándares y las prácticas recomendadas del sector de la seguridad.

Security Hub recopila los datos de seguridad de toda su Cuentas de AWS , elAWSque utilice y los productos de socios de terceros compatibles. Le ayuda a analizar sus tendencias de seguridad y a identificar los problemas de seguridad de mayor prioridad.

Cuando utiliza Security Hub yAWS Organizations, puede habilitar automáticamente Security Hub para todas sus cuentas, incluidas las cuentas nuevas a medida que se agregan. Esto aumenta la cobertura de las comprobaciones y hallazgos de Security Hub, lo que proporciona una imagen más completa y precisa de su postura general de seguridad.

Para obtener más información acerca de Security Hub, consulte laAWS Security HubGuía del usuario de.

Utilice la siguiente información como ayuda para integrarAWS Security HubporAWS Organizations.

Roles vinculados a servicios creados al habilitar la integración

Los siguientes ejemplos deRol vinculado al servicio deCuando habilita el acceso de confianza se crea automáticamente en la cuenta de administración de su organización. Esta función permite a Security Hub realizar operaciones compatibles dentro de las cuentas de su organización.

Puede eliminar o modificar esta función sólo si deshabilita el acceso de confianza entre el Security Hub y las Organizations, o si quita la cuenta de miembro de la organización.

- `AWSServiceRoleForSecurityHub`

Principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior sólo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios utilizados por Security Hub otorgan acceso a las siguientes entidades de servicio:

- `securityhub.amazonaws.com`

Habilitación del acceso Security Hub

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte.Permisos necesarios para habilitar el acceso de confianza (p. 232).

Cuando designa un administrador delegado para Security Hub, Security Hub habilita automáticamente el acceso de confianza para Security Hub en su organización.

Habilitación de una cuenta de administrador delegado para Security Hub

Cuando designa una cuenta de miembro como administrador delegado para la organización, los usuarios y las funciones de esa cuenta pueden realizar acciones administrativas para Security Hub que, de lo contrario, sólo pueden ser realizadas por usuarios o roles en la cuenta de administración de la organización. Esto le ayuda a separar la administración de la organización de la gestión de Security Hub.

Para obtener información, consulteDesignación de una cuenta de administrador de Security Huben laAWS Security HubGuía del usuario de.

Para designar una cuenta de miembro como administrador delegado para Security Hub

1. Inicie sesión con su cuenta de administración de Organizations.
2. Lleve a cabo una de las siguientes operaciones:
   - Si su cuenta de administración no tiene habilitado Security Hub, en la consola de Security Hub, elijaIr a Security Hub.
   - Si su cuenta de administración tiene habilitado Security Hub, en la consola de Security Hub, elijaConfiguración.
3. UNDERAdministrador delegado, escriba el ID de la cuenta.

Amazon S3 Storage Lens yAWS Organizations

Al proporcionar a Amazon S3 Storage Lens un acceso confiable a su organización, le permite recopilar y agregar métricas en todos los Cuentas de AWS En su organización, S3 Storage Lens hace esto accediendo a la lista de cuentas que pertenecen a su organización y recopila y analiza las métricas de almacenamiento y uso y actividad de todas ellas.

Para obtener más información, consulte . Para obtener más información, consulte laUso de roles vinculados a servicios para Amazon S3 Storage Lensen laGuía del usuario de Amazon S3 Storage Lens.

Utilice la información siguiente para ayudarle a integrar Amazon S3 Storage Lens conAWS Organizations.

Rol vinculado al servicio creado cuando habilita la integración

Los siguientes ejemplos deRol vinculado al servicio deCuando habilita el acceso de confianza se crea automáticamente en la cuenta de administración de su organización. Esta función permite a Amazon S3 Storage Lens realizar operaciones compatibles en las cuentas de su organización.

Puede eliminar o modificar esta función solo si deshabilita el acceso de confianza entre Amazon S3 Storage Lens y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForS3StorageLens`

Principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior sólo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Las funciones vinculadas a servicios utilizadas por Amazon S3 Storage Lens otorgan acceso a las siguientes entidades principales de servicios:

- `storage-lens.s3.amazonaws.com`

Para habilitar el acceso de confianza con Amazon S3 Storage Lens

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte.Permisos necesarios para habilitar el acceso de confianza (p. 232).

Puede habilitar el acceso de confianza mediante la consola de Amazon S3 Storage Lens de o laAWS Organizationsconsola de .

> **Important**
>
> Le recomendamos encarecidamente que, siempre que sea posible, utilice la consola o las herramientas de Amazon S3 Storage Lens para habilitar la integración con las Organizations. Esto permite a Amazon S3 Storage Lens realizar cualquier configuración que requiera, como la creación de los recursos necesarios para el servicio. Siga estos pasos solo si no puede habilitar la integración mediante las herramientas proporcionadas por Amazon S3 Storage Lens.Para obtener más información, consulteesta nota (p. 232).
> Si habilita el acceso de confianza mediante la consola o las herramientas de Amazon S3 Storage Lens, no necesita completar estos pasos.

Para habilitar el acceso de confianza mediante la consola de Amazon S3

ConsulteCómo habilitar el acceso de confianzaen laAmazon Simple Storage Service Developer Guide.

Puede habilitar el acceso de confianza mediante laAWS Organizations, ejecutando unaAWS CLI, o llamando a una operación de API en uno de losAWSSDK de.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaServiciosEn la página, busque la fila deAmazon S3 Storage Lens, elija el nombre del servicio y, a continuación, elijaHabilitación del acceso de.

3. En el cuadro de diálogo de confirmación, habiliteMostrar la opción para habilitar el acceso de confianza, introduzca**`enable`**En el cuadro y, a continuación, elija.Habilitación del acceso de.
4. Si usted es el administrador de sóloAWS Organizations, dígale al administrador de Amazon S3 Storage Lens de que ahora puede habilitar ese servicio mediante su consola para que funcione conAWS Organizations.

AWS CLI, AWS API

Para habilitar el acceso al servicio de confianza mediante Organizationscli/SDK

Puede utilizar las siguientes:AWS CLIPara habilitar el acceso del servicio de confianza:

- AWS CLI:enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitar Amazon S3 Storage Lens como un servicio de confianza con las Organizations.

```
$ aws organizations enable-aws-service-access \
    --service-principal storage-lens.s3.amazonaws.com
```

  Este comando no genera ninguna salida cuando se realiza correctamente.
- API de AWS: EnableAWSServiceAccess

Deshabilitación del acceso de confianza con Amazon S3 Storage Lens

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consultePermisos necesarios para deshabilitar el acceso de confianza (p. 233).

Puede deshabilitar el acceso de confianza mediante sólo las herramientas de Amazon S3 Storage Lens.

Puede deshabilitar el acceso de confianza mediante la consola de Amazon S3, laAWSCLI o cualquiera de losAWSSDK de.

Para deshabilitar el acceso de confianza mediante la consola de Amazon S3

ConsulteCómo deshabilitar el acceso de confianzaen laAmazon Simple Storage Service Developer Guide.

Para habilitar una cuenta de administrador delegado para Amazon S3 Storage Lens

Cuando designa una cuenta de miembro como administrador delegado para la organización, los usuarios y las funciones de esa cuenta pueden realizar acciones administrativas para Amazon S3 Storage Lens que, de lo contrario, sólo pueden realizar usuarios o roles en la cuenta de administración de la organización. Esto le ayuda a separar la administración de la organización de la administración de Amazon S3 Storage Lens.

Permisos mínimos

Sólo un usuario o rol de IAM en la cuenta de administración de Organizations con el siguiente permiso puede configurar una cuenta de miembro como administrador delegado para Amazon S3 Storage Lens en la organización:
`organizations:RegisterDelegatedAdministrator`
`organizations:DeregisterDelegatedAdministrator`

Amazon S3 Storage Lens admite un máximo de 5 cuentas de administrador delegadas en su organización.

Para designar una cuenta miembro como administrador delegado para Amazon S3 Storage Lens

Puede registrar un administrador delegado mediante la consola de Amazon S3, elAWSCLI o cualquiera de losAWSSDK de. Para registrar una cuenta de miembro como una cuenta de administrador delegado de su organización mediante la consola de Amazon S3, consulteRegistro de un administrador delegadoen laAmazon Simple Storage Service Developer Guide.

Para anular el registro de un administrador delegado para Amazon S3 Storage Lens

Puede anular el registro de un administrador delegado mediante la consola de Amazon S3, laAWSCLI o cualquiera de losAWSSDK de. Para anular el registro de un administrador delegado mediante la consola de Amazon S3, consulteCómo anular el registro de un administrador delegadoen laAmazon Simple Storage Service Developer Guide.

AWS Service Catalog y AWS Organizations

AWS Service Catalog le permite crear y administrar catálogos de servicios de TI aprobados para su uso en AWS.

La integración de AWS Service Catalog con AWS Organizations simplifica el uso compartido de carteras de productos y la copia de productos en una organización. Los administradores de AWS Service Catalog pueden hacer referencia a una organización existente en AWS Organizations al compartir una cartera de productos y pueden compartir la cartera de productos con cualquier unidad organizativa (UO) de confianza en la estructura de árbol de la organización. De este modo desaparece la necesidad de compartir los ID de cartera y que la cuenta de recepción tenga que hacer referencia manualmente al ID de la cartera al importar la cartera. Las carteras compartidas a través de este mecanismo se enumeran en la cuenta de uso compartido en la vista Cartera importada del administrador en AWS Service Catalog.

Para obtener más información acerca deAWS Service Catalog, consulte elAWS Service CatalogGuía del administrador de.

Utilice la siguiente información como ayuda para integrarAWS Service CatalogporAWS Organizations.

Roles vinculados a servicios creados al habilitar la integración

AWS Service Catalogno crea ningún rol vinculado al servicio como parte de habilitar el acceso de confianza.

Entidades de servicio utilizadas para conceder permisos

Para habilitar el acceso de confianza, debe especificar la entidad de servicio siguiente:

- `servicecatalog.amazonaws.com`

Para habilitar el acceso de confianza conAWS Service Catalog

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte.Permisos necesarios para habilitar el acceso de confianza (p. 232).

Puede habilitar el acceso de confianza mediante la consola de AWS Service Catalog o la consola de AWS Organizations.

> Important
>
> Le recomendamos que, en la medida de lo posible, utilice elAWS Service Catalogo herramientas para habilitar la integración con Organizations. Esto le permiteAWS Service Catalogrealizar

cualquier configuración que requiera, como la creación de los recursos necesarios para el servicio. Continúe con estos pasos solo si no puede habilitar la integración utilizando las herramientas proporcionadas porAWS Service CatalogPara obtener más información, consulte.esta nota (p. 232).
Si habilita el acceso de confianza mediante elAWS Service CatalogConsola de la o las herramientas no necesita completar estos pasos.

Para habilitar el acceso de confianza a través de laAWS Service CatalogCLI oAWSSDK

Llame a uno de los siguientes comandos u operaciones:

- AWS CLI:aws servicecatalog enable-aws-organizations-access
- AWSSDK de: AWSServiceCatalog# EnableAWSOrganizationsAccess

Puede habilitar el acceso de confianza mediante laAWS Organizations, ejecutando unaAWS CLI, o llamando a una operación de API en uno de losAWSSDK de.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaServiciosEn la página, busque la fila deAWS Service Catalog, elija el nombre del servicio y, a continuación, elijaHabilitación del acceso de.
3. En el cuadro de diálogo de confirmación, habiliteMostrar la opción para habilitar el acceso de confianza, introduzca**`enable`**En el cuadro y, a continuación, elija.Habilitación del acceso de.
4. Si usted es el administrador de sóloAWS Organizations, dígale al administrador deAWS Service Catalogque ahora pueden habilitar ese servicio usando su consola para trabajar conAWS Organizations.

AWS CLI, AWS API

Para habilitar el acceso al servicio de confianza mediante Organizationscli/SDK

Puede utilizar las siguientes:AWS CLIPara habilitar el acceso del servicio de confianza:

- AWS CLI:enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitarAWS Service CatalogHabilitar como servicio de confianza con las Organizations.

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

  Este comando no genera ninguna salida cuando se realiza correctamente.
- API de AWS: EnableAWSServiceAccess

Deshabilitación del acceso de confianza conAWS Service Catalog

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consultePermisos necesarios para deshabilitar el acceso de confianza (p. 233).

Si deshabilita el acceso de confianza mediante AWS Organizations mientras utiliza AWS Service Catalog, los usos compartidos actuales no se eliminan, pero le impide crear nuevos usos compartidos en su organización. Los usos compartidos actuales no se sincronizarán con la estructura de su organización si se cambian después de llamar a esta acción.

Puede deshabilitar el acceso de confianza mediante la herramienta deAWS Service CatalogorAWS OrganizationsHerramientas.

> **Important**
>
> Le recomendamos que, en la medida de lo posible, utilice elAWS Service Catalogo herramientas para deshabilitar la integración con Organizations. Esto le permiteAWS Service Catalogrealizar cualquier limpieza que requiera, como eliminar recursos o roles de acceso que ya no necesite el servicio. Continúe con estos pasos solo si no puede deshabilitar la integración utilizando las herramientas proporcionadas porAWS Service Catalog.
> Si deshabilita el acceso de confianza mediante elAWS Service CatalogConsola de la o las herramientas no necesita completar estos pasos.

Para deshabilitar el acceso de confianza mediante laAWS Service CatalogCLI oAWSSDK

Llame a uno de los siguientes comandos u operaciones:

- AWS CLI:aws servicecatalog enable-aws-organizations-access
- AWSSDK de: DesactivarAwsOrganizationsAccess

Puede deshabilitar el acceso de confianza mediante laAWS Organizations, mediante la ejecución de una OrganizationsAWS CLI, o llamando a una operación de API de Organizations en uno de losAWSSDK de.

AWS Management Console

Para deshabilitar el acceso al servicio de confianza mediante la consola Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaServiciosEn la página, busque la fila deAWS Service Catalogy, a continuación, elija el nombre del servicio.
3. SeleccionarDeshabilitar el acceso de confianza.
4. En el cuadro de diálogo de confirmación, escriba**`disable`**en el cuadro y, a continuación, elija.Deshabilitar el acceso de confianza.
5. Si usted es el administrador de sóloAWS Organizations, dígale al administrador deAWS Service Catalogque ahora pueden deshabilitar ese servicio usando su consola o herramientas para trabajar conAWS Organizations.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante el CLI/SDK de Organizations

Puede utilizar las siguientes:AWS CLIPara deshabilitar el acceso del servicio de confianza:

- AWS CLI:disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitarAWS Service CatalogHabilitar como servicio de confianza con las Organizations.

```
$ aws organizations disable-aws-service-access \
```

```
    --service-principal servicecatalog.amazonaws.com
```

Este comando no genera ninguna salida cuando se realiza correctamente.

- API de AWS: DisableAWSServiceAccess

Service Quotas y AWS Organizations

Service Quotas es un servicio de AWS que le permite ver y administrar sus cuotas desde una ubicación central. Las cuotas, también conocidas como límites, son el valor máximo de los recursos, acciones y elementos de su Cuenta de AWS .

Cuando Service Quotas se asocia a AWS Organizations, puede crear una plantilla de solicitud de cuota para solicitar automáticamente aumentos de cuota cuando se creen las cuentas.

Para obtener más información acerca de Service Quotas, consulte la Guía del usuario de Service Quotas.

Utilice la siguiente información como ayuda para integrar Service Quotas conAWS Organizations.

Roles vinculados a servicios creados al habilitar la integración

Los siguientes ejemplos deRol vinculado al servicio deCuando habilita el acceso de confianza, se crea automáticamente en la cuenta de administración de su organización. Esta función permite que las cuotas de servicio realicen operaciones admitidas dentro de las cuentas de su organización.

Puede eliminar o modificar esta función sólo si deshabilita el acceso de confianza entre las Service Quotas y las Organizations, o si quita la cuenta de miembro de la organización.

- `AWSServiceRoleForServiceQuotas`

Principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior sólo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios utilizados por las Service Quotas otorgan acceso a las siguientes entidades de servicio:

- `servicequotas.amazonaws.com`

Habilitación del acceso de confianza con Service Quotas

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte.Permisos necesarios para habilitar el acceso de confianza (p. 232).

Puede habilitar el acceso de confianza mediante Service Quotas.

Puede habilitar el acceso de confianza mediante la consola Service Quotas

Para habilitar el acceso de confianza mediante la consola Service Quotas

Inicie sesión conAWS OrganizationsPara configurar la plantilla en la consola de Service Quotas. Para obtener más información, consulte Uso de una plantilla de Service Quotas en la Guía del usuario de Service Quotas.

Para habilitar el acceso de confianza mediante las Service QuotasAWS CLISDK de.

Llame al siguiente comando u operación:

- AWS CLI:aws service-quotas associate-service-quota-template
- AWSSDK de: AssociateServiceQuotaTemplate

AWS Single Sign-On y AWS Organizations

AWS Single Sign-On(AWS SSO) proporciona servicios de inicio de sesión único para todos los Cuentas de AWS y aplicaciones en la nube. Se conecta con Microsoft Active Directory a través de AWS Directory Service para permitir a los usuarios de dicho directorio iniciar sesión en un portal de usuario personalizado con sus nombres de usuario y contraseñas de Active Directory. Desde el portal, los usuarios obtienen acceso a todas las Cuentas de AWS y aplicaciones en la nube que proporcione en el portal.

Para obtener más información acerca de AWS SSO, consulte la Guía del usuario de AWS Single Sign-On.

Utilice la siguiente información como ayuda para integrarAWS Single Sign-OnporAWS Organizations.

Roles vinculados a servicios creados al habilitar la integración

Los siguientes ejemplos deRol vinculado al servicio deCuando habilita el acceso de confianza, se crea automáticamente en la cuenta de administración de su organización. Este rol permiteAWS SSOPara realizar operaciones compatibles con las cuentas de su organización.

Puede eliminar o modificar esta función sólo si deshabilita el acceso de confianza entreAWS SSOy Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForSSO`

Principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior sólo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Uso de roles vinculados a servicios deAWS SSOconceder acceso a las siguientes entidades de servicio:

- `sso.amazonaws.com`

Para habilitar el acceso de confianza conAWS SSO

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte.Permisos necesarios para habilitar el acceso de confianza (p. 232).

Puede habilitar el acceso de confianza mediante la consola de AWS Single Sign-On o la consola de AWS Organizations.

> **Important**
>
> Le recomendamos que, en la medida de lo posible, utilice elAWS Single Sign-Ono herramientas para habilitar la integración con Organizations. Esto le permiteAWS Single Sign-Onrealizar cualquier configuración que requiera, como la creación de los recursos necesarios para

el servicio. Continúe con estos pasos solo si no puede habilitar la integración utilizando las herramientas proporcionadas porAWS Single Sign-OnPara obtener más información, consulte.esta nota (p. 232).
Si habilita el acceso de confianza mediante elAWS Single Sign-OnConsola de la o las herramientas no necesita completar estos pasos.

AWS SSOrequiere acceso de confianza conAWS Organizationspara funcionar. El acceso de confianza se habilita al configurar AWS SSO. Para obtener más información, consulteIntroducción - Paso 1: HabilitarAWS Single Sign-Oen laAWS Single Sign-OnGuía del usuario de.

Puede habilitar el acceso de confianza mediante laAWS Organizations, ejecutando unaAWS CLI, o llamando a una operación de API en uno de losAWSSDK de.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaServiciosEn la página, busque la fila deAWS Single Sign-On, elija el nombre del servicio y, a continuación, elijaHabilitación del acceso de.
3. En el cuadro de diálogo de confirmación, habiliteMostrar la opción para habilitar el acceso de confianza, introduzca**`enable`**en el cuadro y, a continuación, elija.Habilitación del acceso de.
4. Si usted es el administrador de sóloAWS Organizations, dígale al administrador deAWS Single Sign-Onque ahora pueden habilitar ese servicio usando su consola para trabajar conAWS Organizations.

AWS CLI, AWS API

Para habilitar el acceso al servicio de confianza mediante Organizationscli/SDK

Puede utilizar las siguientes:AWS CLIPara habilitar el acceso del servicio de confianza:

- AWS CLI:enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitarAWS Single Sign-OnHabilitar como servicio de confianza con las Organizations.

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

  Este comando no genera ninguna salida cuando se realiza correctamente.
- API de AWS: EnableAWSServiceAccess

Deshabilitación del acceso de confianza conAWS SSO

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consultePermisos necesarios para deshabilitar el acceso de confianza (p. 233).

AWS SSOrequiere acceso de confianza conAWS OrganizationsPara operar. Si deshabilita el acceso de confianza con AWS Organizations mientras utiliza AWS SSO, este deja de funcionar porque no puede obtener acceso a la organización. Los usuarios no pueden utilizar AWS SSO para tener acceso a las cuentas. Las funciones creadas por AWS SSO se mantienen, pero el servicio AWS SSO no puede obtener acceso a ellos. Las funciones vinculadas al servicio AWS SSO se mantienen. Si vuelve a habilitar el

acceso de confianza, AWS SSO seguirá funcionando como lo hacía antes sin necesidad de volver a configurar el servicio.

Si elimina una cuenta de su organización, AWS SSO limpia automáticamente los metadatos y los recursos, como su función vinculada al servicio. Una cuenta independiente que se elimina de una organización deja de funcionar con AWS SSO.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza mediante laAWS Organizations, mediante la ejecución de una OrganizationsAWS CLI, o llamando a una operación de API de Organizations en uno de losAWSSDK de.

AWS Management Console

Para deshabilitar el acceso al servicio de confianza mediante la consola Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaServiciosEn la página, busque la fila deAWS Single Sign-Ony, a continuación, elija el nombre del servicio.
3. SeleccionarDeshabilitar el acceso de confianza.
4. En el cuadro de diálogo de confirmación, escriba**`disable`**en el cuadro y, a continuación, elija.Deshabilitar el acceso de confianza.
5. Si usted es el administrador de sóloAWS Organizations, dígale al administrador deAWS Single Sign-Onque ahora pueden deshabilitar ese servicio usando su consola o herramientas para trabajar conAWS Organizations.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante el CLI/SDK de Organizations

Puede utilizar las siguientes:AWS CLIPara deshabilitar el acceso del servicio de confianza:

- AWS CLI:disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitarAWS Single Sign-OnHabilitar como servicio de confianza con las Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal sso.amazonaws.com
```

  Este comando no genera ninguna salida cuando se realiza correctamente.
- API de AWS: DisableAWSServiceAccess

AWS Systems Manager y AWS Organizations

AWS Systems Manager es un conjunto de capacidades que le ofrece control y visibilidad de sus recursos de AWS. Dos de las características que forman parte de Systems Manager pueden trabajar con Organizations para trabajar en todas las Cuentas de AWS En su organización,

- Systems Manager Explorer, es un panel de operaciones personalizable que le ofrece información acerca de suAWSde AWS. Puede sincronizar los datos de las operaciones en todas las Cuentas de AWS en su organización mediante el Explorador de Organizations y Systems Manager. Para obtener más información, consulteExplorador de Systems Manageren laAWS Systems ManagerGuía del usuario de.

- Systems Manager Change Manager es un marco de administración de cambios empresarial para solicitar, aprobar, implementar y generar informes sobre los cambios operativos en la configuración y la infraestructura de la aplicación. Para obtener más información, consulteAWS Systems ManagerAdministrador de cambiosen laAWS Systems ManagerGuía del usuario de.

Utilice la siguiente información como ayuda para integrarAWS Systems ManagerporAWS Organizations.

Roles vinculados a servicios creados al habilitar la integración

Los siguientes ejemplos deRol vinculado al servicio deCuando habilita el acceso de confianza, se crea automáticamente en la cuenta de administración de su organización. Esta función permite a Systems Manager realizar operaciones compatibles dentro de las cuentas de su organización.

Puede eliminar o modificar esta función sólo si deshabilita el acceso de confianza entre Systems Manager y Organizations, o si quita la cuenta de miembro de la organización.

- `AWSServiceRoleForAmazonSSM_AccountDiscovery`

Principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior sólo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios utilizados por Systems Manager otorgan acceso a las siguientes entidades de servicio:

- `ssm.amazonaws.com`

Habilitación del acceso de confianza con Systems Manager

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte.Permisos necesarios para habilitar el acceso de confianza (p. 232).

Puede habilitar el acceso de confianza mediante la consola de AWS Systems Manager o la consola de AWS Organizations.

> **Important**
>
> Le recomendamos que, en la medida de lo posible, utilice elAWS Systems Managero herramientas para habilitar la integración con Organizations. Esto le permiteAWS Systems Managerrealizar cualquier configuración que requiera, como la creación de los recursos necesarios para el servicio. Continúe con estos pasos solo si no puede habilitar la integración utilizando las herramientas proporcionadas porAWS Systems ManagerPara obtener más información, consulte.esta nota (p. 232).
> Si habilita el acceso de confianza mediante elAWS Systems ManagerConsola de la o las herramientas no necesita completar estos pasos.

Para habilitar el acceso de confianza mediante la consola de Systems Manager

Debe iniciar sesión con suAWS OrganizationsPara crear una sincronización de datos de recursos. Para obtener información, consulteConfiguración de Explorer para mostrar datos de varias cuentas y regionesen laAWS Systems ManagerGuía del usuario de.

Puede habilitar el acceso de confianza mediante laAWS Organizations, ejecutando unaAWS CLI, o llamando a una operación de API en uno de losAWSSDK de.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaServiciosEn la página, busque la fila deAWS Systems Manager, elija el nombre del servicio y, a continuación, elijaHabilitación del acceso de.
3. En el cuadro de diálogo de confirmación, habiliteMostrar la opción para habilitar el acceso de confianza, introduzca**`enable`**en el cuadro y, a continuación, elija.Habilitación del acceso de.
4. Si usted es el administrador deAWS Organizations, dígale al administrador deAWS Systems Managerque ahora pueden habilitar ese servicio usando su consola para trabajar conAWS Organizations.

AWS CLI, AWS API

Para habilitar el acceso al servicio de confianza mediante Organizationscli/SDK

Puede utilizar las siguientes:AWS CLIPara habilitar el acceso del servicio de confianza:

- AWS CLI:enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitarAWS Systems ManagerHabilitar como servicio de confianza con las Organizations.

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

  Este comando no genera ninguna salida cuando se realiza correctamente.
- API de AWS: EnableAWSServiceAccess

Deshabilitación del acceso de confianza con Systems Manager

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consultePermisos necesarios para deshabilitar el acceso de confianza (p. 233).

Systems Manager requiere acceso de confianza conAWS Organizationspara sincronizar los datos de operaciones a través de Cuentas de AWS En su organización, Si deshabilita el acceso de confianza, Systems Manager no puede sincronizar los datos de las operaciones e informa sobre un error.

Puede deshabilitar el acceso de confianza mediante la herramienta deAWS Systems ManagerorAWS OrganizationsHerramientas.

Important

Le recomendamos que, en la medida de lo posible, utilice elAWS Systems Managero herramientas para deshabilitar la integración con Organizations. Esto le permiteAWS Systems Managerrealizar cualquier limpieza que requiera, como eliminar recursos o roles de acceso que ya no necesite el servicio. Continúe con estos pasos solo si no puede deshabilitar la integración utilizando las herramientas proporcionadas porAWS Systems Manager.
Si deshabilita el acceso de confianza mediante elAWS Systems ManagerConsola de la o las herramientas no necesita completar estos pasos.

Para deshabilitar el acceso de confianza mediante la consola de Systems Manager

ConsulteEliminación de una sincronización de datos de recursos de Systems Manager Exploreren laAWS Systems ManagerGuía del usuario de. Para habilitar el acceso de confianza de nuevo, tiene que crear una nueva sincronización de datos de recursos para Systems Manager Explorer.

Puede deshabilitar el acceso de confianza mediante laAWS Organizations, mediante la ejecución de una OrganizationsAWS CLI, o llamando a una operación de API de Organizations en uno de losAWSSDK de.

AWS Management Console

Para deshabilitar el acceso al servicio de confianza mediante la consola Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaServiciosEn la página, busque la fila deAWS Systems Managery, a continuación, elija el nombre del servicio.
3. SeleccionarDeshabilitar el acceso de confianza.
4. En el cuadro de diálogo de confirmación, escriba**`disable`**en el cuadro y, a continuación, elija.Deshabilitar el acceso de confianza.
5. Si usted es el administrador deAWS Organizations, dígale al administrador deAWS Systems Managerque ahora pueden deshabilitar ese servicio usando su consola o herramientas para trabajar conAWS Organizations.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante el CLI/SDK de Organizations

Puede utilizar las siguientes:AWS CLIPara deshabilitar el acceso del servicio de confianza:

- AWS CLI:disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitarAWS Systems ManagerHabilitar como servicio de confianza con las Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal ssm.amazonaws.com
```

  Este comando no genera ninguna salida cuando se realiza correctamente.
- API de AWS: DisableAWSServiceAccess

Para habilitar una cuenta de administrador delegado para Systems Manager

Cuando designa una cuenta de miembro como administrador delegado para la organización, los usuarios y las funciones de esa cuenta pueden realizar acciones administrativas para Systems Manager que, de lo contrario, sólo pueden realizar usuarios o roles en la cuenta de administración de la organización. Esto le ayuda a separar la administración de la organización de la administración de Systems Manager.

Si utiliza Change Manager en una organización, utiliza una cuenta de administrador delegada. Este es el Cuenta de AWS que se ha designado como la cuenta para administrar plantillas de cambio, solicitudes de cambio, runbooks de cambios y flujos de trabajo de aprobación en Change Manager. La cuenta delegada administra las actividades de cambio en toda la organización. Cuando configura su organización para utilizarla con Change Manager, especifica cuál de sus cuentas sirve en este rol. No tiene que ser la cuenta de gestión de la organización. La cuenta de administrador delegada no es necesaria si utiliza Change Manager con una sola cuenta.»

Para designar una cuenta de miembro como administrador delegado para Systems Manager

Para el Explorador de Systems Manager, consulteConfiguración de un administrador delegadoen laAWS Systems ManagerGuía del usuario de.

Para Systems Manager Change Manager, consulteConfiguración de una organización y una cuenta delegada para Change Manageren laAWS Systems ManagerGuía del usuario de.

Políticas de etiquetas y AWS Organizations

Políticas de etiquetasson un tipo de directiva enAWS OrganizationsDe este modo, podrá estandarizar las etiquetas en los recursos de las cuentas de su organización. Para obtener más información acerca de las políticas de etiquetas, consulte Políticas de etiquetas (p. 195).

Utilice la siguiente información como ayuda para integrar las directivas de etiquetas conAWS Organizations.

Principales de servicios utilizados por los roles vinculados a servicios

Las Organizations interactúan con las etiquetas adjuntas a los recursos mediante la siguiente entidad de servicio.

- `tagpolicies.tag.amazonaws.com`

Habilitación del acceso de confianza para directivas de

Puede habilitar el acceso de confianza mediante la habilitación de directivas de etiquetas en la organización o mediante elAWS Organizationsconsola de .

> **Important**
>
> Recomendamos encarecidamente que habilite el acceso de confianza mediante directivas de etiquetas. Esto permite a las Organizations realizar las tareas de configuración necesarias.

Puede habilitar el acceso de confianza para las directivas de etiquetas habilitando el tipo de directiva de etiqueta en el cuadroAWS Organizationsconsola de . Para obtener más información, consulte Para habilitar un tipo de política (p. 87) .

Puede habilitar el acceso de confianza mediante laAWS Organizations, ejecutando unaAWS CLI, o llamando a una operación de API en uno de losAWSSDK de.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir una función de IAM o iniciar sesión como usuario raíz (No recomendado) en la cuenta de gestión de la organización.
2. En la páginaServiciosEn la página, busque la fila dePolíticas de etiquetas, elija el nombre del servicio y, a continuación, elijaHabilitación del acceso de.
3. En el cuadro de diálogo de confirmación, habiliteMostrar la opción para habilitar el acceso de confianza, introduzca**`enable`**en el cuadro y, a continuación, elija.Deshabilitar el acceso de confianza.
4. Si usted es el administrador deAWS Organizations, dígale al administrador de las políticas de etiquetas de que ahora puede habilitar ese servicio mediante su consola para que funcione conAWS Organizations.

AWS CLI, AWS API

Para habilitar el acceso al servicio de confianza mediante Organizationscli/SDK

Puede utilizar las siguientes:AWS CLIPara habilitar el acceso del servicio de confianza:

- AWS CLI:enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitar directivas de etiquetas como un servicio de confianza con Organizations.

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

  Este comando no genera ninguna salida cuando se realiza correctamente.
- API de AWS: EnableAWSServiceAccess

Para deshabilitar el acceso de confianza con directivas de etiquetas,

Puede deshabilitar el acceso de confianza para las directivas de etiquetas deshabilitando el tipo de directiva de etiqueta en el cuadroAWS Organizationsconsola de . Para obtener más información, consulte Deshabilitar un tipo de política (p. 88) .

AWS Trusted Advisor y AWS Organizations

AWS Trusted AdvisorInspeccione elAWSy realiza recomendaciones cuando surge la oportunidad de ahorrar dinero, mejorar el desempeño y la disponibilidad del sistema o ayudar a cerrar los errores de seguridad. Cuando se integra con las Organizations, puede recibirTrusted Advisorcompruebe los resultados de todas las cuentas de su organización y descargue informes para ver los resúmenes de sus comprobaciones y los recursos afectados.

Para obtener más información, consulteVista organizativa paraAWS Trusted Advisoren laAWS SupportGuía del usuario de.

Utilice la siguiente información como ayuda para integrarAWS Trusted AdvisorporAWS Organizations.

Roles vinculados a servicios creados al habilitar la integración

Los siguientes ejemplos deRol vinculado al servicio deCuando habilita el acceso de confianza, se crea automáticamente en la cuenta de administración de su organización. Este rol permiteTrusted AdvisorPara realizar operaciones compatibles con las cuentas de su organización.

Puede eliminar o modificar esta función sólo si deshabilita el acceso de confianza entreTrusted Advisory Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForTrustedAdvisorReporting`

Principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior sólo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Uso de roles vinculados a servicios deTrusted Advisorconceder acceso a las siguientes entidades de servicio:

- `reporting.trustedadvisor.amazonaws.com`

Para habilitar el acceso de confianza conTrusted Advisor

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte.Permisos necesarios para habilitar el acceso de confianza (p. 232).

Puede habilitar el acceso de confianza medianteAWS Trusted Advisor.

Para habilitar el acceso de confianza a través de laTrusted Advisorconsole

ConsulteHabilitar vista organizativaen laAWS SupportGuía del usuario de.

Deshabilitación del acceso de confianza conTrusted Advisor

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consultePermisos necesarios para deshabilitar el acceso de confianza (p. 233).

Después de deshabilitar esta característica,Trusted AdvisorDetiene el registro de información de comprobación para todas las demás cuentas de su organización. No puede ver ni descargar informes existentes ni crear informes nuevos.

Puede deshabilitar el acceso de confianza mediante la herramienta deAWS Trusted AdvisororAWS OrganizationsHerramientas.

> Important
>
> Le recomendamos que, en la medida de lo posible, utilice elAWS Trusted Advisoro herramientas para deshabilitar la integración con Organizations. Esto le permiteAWS Trusted Advisorrealizar cualquier limpieza que requiera, como eliminar recursos o roles de acceso que ya no necesite el servicio. Continúe con estos pasos solo si no puede deshabilitar la integración utilizando las herramientas proporcionadas porAWS Trusted Advisor.
> Si deshabilita el acceso de confianza mediante elAWS Trusted AdvisorConsola de la o las herramientas no necesita completar estos pasos.

Para deshabilitar el acceso de confianza mediante laTrusted Advisorconsole

ConsulteDeshabilitación de la vistaen laAWS SupportGuía del usuario de.

Puede deshabilitar el acceso de confianza ejecutando una OrganizationsAWS CLI, o llamando a una operación de API de Organizations en uno de losAWSSDK de.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante el CLI/SDK de Organizations

Puede utilizar las siguientes:AWS CLIPara deshabilitar el acceso del servicio de confianza:

- AWS CLI:disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitarAWS Trusted AdvisorHabilitar como servicio de confianza con las Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal reporting.trustedadvisor.amazonaws.com
```

  Este comando no genera ninguna salida cuando se realiza correctamente.
- API de AWS: DisableAWSServiceAccess

Seguridad en AWS Organizations

La seguridad en la nube de AWS es la mayor prioridad. Como cliente de AWS, se beneficiará de una arquitectura de red y un centro de datos diseñados 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–AWSes responsable de proteger la infraestructura que ejecutaAWSen elAWSEn la nube.AWSTambién le proporciona servicios que puede utilizar de forma segura. Auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información acerca de los programas de conformidad que se aplican a AWS Organizations, consulte Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube— Su responsabilidad está determinada por elAWSque 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 utilizan Organizations. En los siguientes temas, se le mostrará cómo configurar las Organizations para que cumplan sus objetivos de seguridad y conformidad. También aprenderá a utilizar otrosAWSque le ayudan a monitorear y proteger los recursos de sus Organizations.

Temas

AWS Identity and Access Management y AWS Organizations

El acceso a AWS Organizations requiere credenciales. Estas credenciales deben tener permisos para obtener acceso aAWSComo un bucket de Amazon Simple Storage Service (Amazon S3), una instancia de Amazon Elastic Compute Cloud (Amazon EC2) o unAWS OrganizationsLa unidad organizativa (OU). En las siguientes secciones presentamos más detalles sobre cómo utilizarAWS Identity and Access ManagementPara ayudar a proteger el acceso a su organización y controlar quién puede administrarla.

Para determinar quién puede administrar qué partes de su organización,AWS Organizationsutiliza el mismo modelo de permisos basados en IAM que otrosAWSServicios de . Como administrador de la cuenta de administración de una organización, puede conceder permisos basados en IAM para realizarAWS OrganizationsPara asociar políticas a usuarios, grupos y funciones de en la cuenta de administración. Estas políticas especifican las acciones que pueden realizar esas entidades. Puede asociar una política de permisos de IAM a un grupo del que el usuario es miembro o directamente a un usuario o función. Como

práctica recomendada, es conveniente que asocie las políticas a grupos en lugar de a usuarios. También tiene la opción de conceder permisos completos de administrador a otros usuarios.

Para la mayoría de las operaciones de administrador paraAWS Organizations, tendrá que asociar permisos a los usuarios o grupos en la cuenta de administración. Si un usuario de una cuenta miembro debe realizar operaciones de administrador para su organización, tendrá que conceder laAWS Organizationspermisos para unaRol de IAMen la cuenta de administración y permitir que el usuario de la cuenta de miembro asuma el rol. Para obtener información general acerca de las políticas de permisos de IAM, consulteDescripción general de políticas de IAMen laGuía del usuario de IAM.

Temas

Authentication

Puede obtener acceso a AWS con los siguientes tipos de identidades:

- Cuenta de AWS Usuario raíz— Cuando se inscriba enAWS, proporciona una dirección de correo electrónico y la contraseña asociada a su Cuenta de AWS . Estas son las credenciales raíz y proporcionan acceso completo a todos los recursos de AWS.

  > **Important**
  >
  > Por razones de seguridad, recomendamos que utilice las credenciales de usuario raíz solo para crear unaUsuario administrador de, que es unaUsuario de IAMcon permisos completos a su Cuenta de AWS . Después, podrá utilizar este usuario administrador para crear otros usuarios y funciones de IAM con permisos limitados. Para obtener más información, consultePrácticas recomendadas de IAMyCreación del primer grupo y usuario administrador de IAMen laGuía del usuario de IAM.

- Usuario de IAM— UnUsuario de IAMes simplemente una identidad dentro de su Cuenta de AWS Con permisos personalizados específicos (por ejemplo, permisos para crear un sistema de archivos en Amazon Elastic File System). Puede utilizar un nombre de usuario y contraseña de IAM para iniciar sesión y protegerAWSLas páginas web comoAWS Management Console,AWSForos de debate de, o elAWSCentro de soporte de.

  Además de un nombre de usuario y una contraseña, puede generar claves de acceso para cada usuario. Puede utilizar estas claves cuando obtenga acceso a los servicios de AWS mediante programación, ya sea a través de uno de los SDK o mediante la AWS Command Line Interface (AWS CLI). El SDK y las herramientas de la AWS CLI usan claves de acceso para firmar criptográficamente la solicitud. Si no utiliza las herramientas de AWS, debe firmar la solicitud. AWS Organizations es compatible con Signature Version 4, un protocolo para autenticar solicitudes entrantes de la API. Para obtener más información acerca de la autenticación de solicitudes, consulteProceso de firma Signature Version 4en laAWSReferencia general de.

- Rol de IAM: un rol de IAM es otra identidad de IAM que puede crear en la cuenta que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una persona determinada. Un rol de IAM le permite obtener claves de acceso temporal que se pueden utilizar para obtenerAWSservicios y recursos de. Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:
  - Acceso de usuarios federados: en lugar de crear un usuario de IAM, puede usar identidades de usuario preexistentes deAWS Directory Service, el directorio de usuarios de la compañía o un proveedor de identidades web. A estas identidades se les llama usuarios federados. AWS asigna una función a un usuario federado cuando se solicita acceso a través de un proveedor de identidad. Para

obtener más información acerca de los usuarios federados, consulte Usuarios federados y roles en la Guía del usuario de IAM.

- Acceso entre cuentas: puede utilizar un rol de IAM en su cuenta para conceder otro Cuenta de AWS para acceder a los recursos de su cuenta. Para ver un ejemplo, consulte .Tutorial: Delegar el acceso entre Cuentas de AWS Uso de roles de IAMen laGuía del usuario de IAM.
- AWSAcceso a servicios de :: puede utilizar un rol de IAM en su cuenta para conceder unaAWSPara obtener acceso a los recursos de su cuenta. Por ejemplo, puede crear una función que permita a Amazon Redshift obtener acceso a un bucket de Amazon S3 en su nombre y, a continuación, cargar los datos almacenados en el bucket en un clúster de Amazon Redshift. Para obtener más información, consulteCreación de un rol para delegar permisos a unAWSService (Servicio)en laGuía del usuario de IAM.
- Aplicaciones que se ejecutan en Amazon EC2: en lugar de almacenar claves de acceso en la instancia EC2 para que las usen aplicaciones que se ejecutan en la instancia y queAWSPuede utilizar un rol de IAM para administrar credenciales temporales para estas aplicaciones. Para asignar una función de AWS a una instancia EC2 y ponerla a disposición de todas las aplicaciones, cree un perfil de instancia asociado a dicha instancia. Un perfil de instancia contiene la función y permite a los programas que se encuentran en ejecución en la instancia EC2 obtener credenciales temporales. Para obtener más información, consulte Uso de roles para aplicaciones en Amazon EC2 en la Guía del usuario de IAM.

Control de acceso

Puede tener credenciales válidas para autenticar las solicitudes, pero a menos que tenga permisos no podrá administrar o tener acceso a los recursos de AWS Organizations. Por ejemplo, debe tener permisos para crear una unidad organizativa o para asociar una política de control de servicios (SCP) (p. 108) a una cuenta.

En las secciones siguientes, se describe cómo administrar los permisos de AWS Organizations.

- Administración de permisos en su organización de AWS (p. 309)
- Usar políticas basadas en identidad (políticas de IAM) paraAWS Organizations (p. 315)
- Control de acceso basado en atributos con etiquetas yAWS Organizations (p. 318)

Administración de permisos en su organización de AWS

All (Todos)AWSTodos los recursos de, incluidos los nodos raíz, las unidades organizativas, las unidades organizativas, las cuentas y las políticas de una organización son propiedad de Cuenta de AWS Y los permisos para crear o tener acceso a un recurso se rigen por las políticas de permisos. Para una organización, su cuenta de administración posee todos los recursos. Un administrador de la cuenta puede controlar el acceso a los recursos de AWS asociando políticas de permisos a las identidades de IAM (usuarios, grupos y funciones).

> Note
>
> Un administrador de la cuenta (o usuario administrador) es un usuario con permisos de administrador. Para obtener más información, consulte Prácticas recomendadas de IAM en la Guía del usuario de IAM.

Cuando concede permisos, decide quién debe obtener los permisos, para qué recursos se obtienen permisos y qué acciones específicas desea permitir en esos recursos.

De forma predeterminada, los usuarios, grupos y roles de IAM no tienen permisos. Como administrador de la cuenta de administración de una organización, puede realizar tareas administrativas o delegar permisos

de administrador a otros usuarios o funciones de IAM en la cuenta de administración. Para ello, asocia una política de permisos de IAM a un usuario, grupo o función de IAM. De forma predeterminada, un usuario no tiene ningún permiso; esto recibe el nombre de denegación implícita. La política invalida la denegación implícita con un permiso explícito que especifica las acciones que puede realizar el usuario y los recursos que puede utilizar en las acciones. Si los permisos se conceden a un rol, los usuarios de otras cuentas de la organización pueden asumir ese rol.

Recursos y operaciones de AWS Organizations

En esta sección se explica cómoAWS OrganizationsSe corresponden con los conceptos equivalentes de IAM.

Resources

En AWS Organizations, puede controlar el acceso a los siguientes recursos:

- La raíz y las unidades organizativas que componen la estructura jerárquica de una organización.
- Las cuentas que son miembros de la organización
- Las políticas que adjunta a las entidades de la organización
- Los protocolos que usa para cambiar el estado de la organización

Cada uno de esos recursos tiene un único nombre de recurso de Amazon (ARN) asociado. El acceso a un recurso se controla especificando su ARN en la`Resource`elemento de una política de permisos de IAM. Para obtener una lista completa de los formatos de ARN para los recursos que se utilizan enAWS Organizations, consulteRecursos definidos porAWS Organizationsen laGuía del usuario de IAM.

Operations

AWS ofrece un conjunto de operaciones para trabajar con los recursos de una organización. Estas operaciones le permiten realizar tareas como crear, mostrar, modificar y eliminar recursos y obtener acceso a su contenido. Se puede hacer referencia a la mayoría de las operaciones en la`Action`Elemento de una política de IAM para controlar quién puede utilizar dicha operación. Para obtener una lista deAWS OrganizationsLas operaciones que se pueden utilizar como permisos en una política de IAM, consultePermisos de acción de API definidos porAWSOrganizacionesen laGuía del usuario de IAM.

Al combinar un elemento `Action` y un elemento `Resource` en el elemento `Statement` de una política de permisos, puede controlar exactamente qué recursos de ese conjunto concreto de acciones se pueden usar.

Claves de condición

AWS ofrece claves de condición que se pueden consultar para proporcionar un control más detallado de determinadas acciones. Puede hacer referencia a estas claves de condición en el`Condition`Effect elemento de una política de IAM para especificar las circunstancias adicionales que se deben cumplir para poder considerar una coincidencia.

Las siguientes claves de condición son especialmente útiles con AWS Organizations:

- `aws:PrincipalOrgID`— Simplifica la especificación`Principal`Elemento en una política basada en recursos. Esta clave global proporciona una alternativa a mostrar todos los ID de todas las cuentas de Cuentas de AWS En una organización. En lugar de mostrar todas las cuentas de la organización, puede especificar el ID de organización (p. 45) en el elemento `Condition`.

  Note

  Esta condición global también se aplica a la cuenta de administración de una organización.

Para obtener más información, consulte la descripción de`PrincipalOrgID`inAWSClaves de contexto de condición globales deen laGuía del usuario de IAM.

- `aws:PrincipalOrgPaths`: utilice esta clave de condición para hacer coincidir los miembros de una raíz de organización específica, una unidad organizativa o sus hijos. La`aws:PrincipalOrgPaths`La clave de condición devuelve verdadera cuando el elemento principal (usuario raíz, usuario de IAM o rol) que realiza la solicitud se encuentra en la ruta de la organización especificada. Una ruta es una representación de texto de la estructura de una entidad de AWS Organizations. Para obtener más información acerca de las rutas de acceso, consulteDescripción delAWS OrganizationsRuta de la entidaden laGuía del usuario de IAM. Para obtener más información acerca del uso de esta clave de condición, consulteaws:principalOrgPathsen laGuía del usuario de IAM.

  Por ejemplo, el siguiente elemento de condición coincide con los miembros de cualquiera de las dos unidades organizativas de la misma organización.

```
            "Condition": {
                "ForAnyValue:StringLike": {
                    "aws:PrincipalOrgPaths": [
                        "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/",
                        "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-jkl0-awsddddd/"
                    ]
                }
            }
```

- `organizations:PolicyType`: puede utilizar esta clave de condición para restringir las operaciones de API relacionadas con la directiva Organizations para que funcionen únicamente en directivas de Organizations del tipo especificado. Puede aplicar esta clave de condición a cualquier instrucción de política que incluya una acción que interactúe con las políticas de la organización.

  Puede utilizar los siguientes valores con esta clave de condición:

  - `AISERVICES_OPT_OUT_POLICY`
  - `BACKUP_POLICY`
  - `SERVICE_CONTROL_POLICY`
  - `TAG_POLICY`

  Por ejemplo, la siguiente política de ejemplo permite al usuario realizar cualquier operación de Organizations. Sin embargo, si el usuario realiza una operación que toma un argumento de política, la operación solo se permite si la política especificada es una política de etiquetado. La operación produce un error si el usuario especifica cualquier otro tipo de política.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "IfTaggingAPIThenAllowOnOnlyTaggingPolicies",
            "Effect": "Allow",
            "Action": "organizations:*",
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": [ "TAG_POLICY" ]
                }
            }
        }
    ]
}
```

- `organizations:ServicePrincipal`— Disponible como condición si se utiliza elEnableAWSServiceAccessorDisableAWSServiceAccesspara habilitar o desactivarlo.acceso de

confianza (p. 232)con otrosAWSServicios de . Puede utilizar `organizations:ServicePrincipal` para limitar las solicitudes que esas operaciones realizan a una lista de nombres de principal de servicio aprobados.

Por ejemplo, la siguiente política permite al usuario especificar solo AWS Firewall Manager cuando habilita y deshabilita el acceso de confianza con AWS Organizations.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowOnlyAWSFirewallIntegration",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [ "fms.amazonaws.com" ]
                }
            }
        }
    ]
}
```

Para ver una lista de todos losAWS Organizations: claves de condición específicas que se pueden utilizar como permisos en una política de IAM, consulteClaves de contexto de condiciónAWS Organizationsen laGuía del usuario de IAM.

Titularidad de los recursos

La Cuenta de AWS Es la propietaria de los recursos que se crean en la cuenta, independientemente de quién los haya creado. En concreto, el propietario del recurso es la Cuenta de AWS de laentidad principal(es decir, la cuenta raíz, un usuario de IAM o un rol de IAM) que autentica la solicitud de creación de recursos. Para unAWSorganización, es decirSiemprela cuenta de gestión. No puede llamar a la mayoría de las operaciones que crean o tiene acceso a los recursos de la organización desde las cuentas miembro. Los siguientes ejemplos ilustran cómo funciona:

- Si utiliza las credenciales de cuenta raíz de su cuenta de administración para crear una unidad organizativa, su cuenta de administración será la propietaria del recurso. (En AWS Organizations, el recurso es la unidad organizativa).
- Si crea un usuario de IAM en su cuenta de administración y concede permisos para crear una unidad organizativa a dicho usuario, el usuario podrá crear una unidad organizativa. Sin embargo, la cuenta de administración, a la que pertenece el usuario, será la propietaria del recurso de unidad organizativa.
- Si crea un rol de IAM en su cuenta de administración con permisos para crear unidades organizativas, cualquier persona puede asumir el rol crearlas. La cuenta de administración, a la que pertenece la función (y no el usuario que la asume) es la propietaria del recurso de unidad organizativa.

Administración del acceso a los recursos

Una política de permisos describe quién tiene acceso a qué. En la siguiente sección se explican las opciones disponibles para crear políticas de permisos.

> **Note**
>
> En esta sección se explica el uso de IAM en el contexto de AWS Organizations. No se proporciona información detallada sobre el servicio de IAM. Para ver la documentación completa de IAM, consulte la Guía del usuario de IAM. Para obtener más información acerca de la sintaxis y descripciones de las políticas de IAM, consulte laReferencia de políticas JSON de IAMen laGuía del usuario de IAM.

Las políticas que se asocian a una identidad de IAM se denominanbasado en identidadesPolíticas (políticas de IAM). Las políticas que se asocian a un recurso se denominanbasado en recursos dePolíticas de.AWS Organizationssolo admite políticas basadas en identidad (políticas de IAM).

Temas

- Políticas de permisos basadas en identidad (políticas de IAM) (p. 313)
- Políticas basadas en recursos (p. 314)

Políticas de permisos basadas en identidad (políticas de IAM)

Puede asociar políticas a identidades de IAM para permitir que esas identidades realicen operaciones enAWSde AWS. Por ejemplo, puede hacer lo siguiente:

- Asociar una política de permisos a un usuario o grupo de su cuenta— Para conceder a un usuario permisos para crear unAWS Organizations, comoaPolítica de control de servicios (SCP) (p. 108)orUna unidad organizativa, puede asociar una política de permisos a un usuario o grupo al que pertenezca el usuario. El usuario o grupo debe estar en la organización de la cuenta de administración.
- Asociar una política de permisos a un rol (conceder permisos entre cuentas): puede asociar una política de permisos basada en identidad a un rol de IAM para conceder acceso entre cuentas a una organización. Por ejemplo, el administrador de la cuenta de administración puede crear un rol para conceder permisos entre cuentas a un usuario de una cuenta miembro de la siguiente manera:
  1. El administrador de la cuenta de administración crea una función de IAM y asocia una política de permisos a la función, que concede permisos a los recursos de la organización.
  2. El administrador de la cuenta de administración asocia una política de confianza al rol que identifica el ID de la cuenta miembro como`Principal`¿Quién puede asumir el rol?
  3. El administrador de la cuenta miembro puede delegar entonces permisos para asumir el rol a cualquier usuario de la cuenta miembro. Esto permite a los usuarios de la cuenta miembro crear o tener acceso a los recursos de la cuenta de administración y la organización. La entidad principal de la política de confianza también puede ser una entidad principal de un servicio de AWS, si desea conceder permisos a un servicio de AWS para que asuma la función.

  Para obtener más información acerca del uso de IAM para delegar permisos, consulteAdministración de accesosen laGuía del usuario de IAM.

A continuación se ofrece un ejemplo de política que permite a un usuario realizar la acción `CreateAccount` en su organización.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid" : "Stmt1OrgPermissions",
            "Effect": "Allow",
            "Action": [
                "organizations:CreateAccount"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

Para obtener más información sobre usuarios, grupos, roles y permisos, consulte Identidades (usuarios, grupos y roles) en la Guía del usuario de IAM.

Políticas basadas en recursos

Algunos servicios, como Amazon S3, admiten políticas de permisos basadas en recursos. Por ejemplo, puede asociar una política a un bucket de Amazon S3 para administrar los permisos de acceso a dicho bucket.AWS Organizationsno admite actualmente políticas basadas en recursos.

Especificación de elementos de política: Acciones, condiciones, efectos y recursos

Para cada recurso de AWS Organizations, el servicio define un conjunto de operaciones de API o acciones, que pueden interactuar con el recurso o manipularlo de algún modo. Para conceder permisos a estas operaciones. AWS Organizations define un conjunto de acciones que puede especificar en una política. Por ejemplo, en el caso del recurso de unidad organizativa; AWS Organizations define acciones como las siguientes:

- `AttachPolicy` y `DetachPolicy`
- `CreateOrganizationalUnit` y `DeleteOrganizationalUnit`
- `ListOrganizationalUnits` y `DescribeOrganizationalUnit`

En algunos casos, la ejecución de una operación de la API podría requerir permisos para más de una acción y podría necesitar permisos para más de un recurso.

A continuación se indican los aspectos más básicos que puede utilizar en una política de permisos de IAM:

- Acción: utilice esta palabra clave para identificar las operaciones (acciones) que desea permitir o denegar. Por ejemplo, en función del elemento `Effect` especificado, `organizations:CreateAccount` permite o deniega los permisos de usuario para realizar la operación `CreateAccount` de AWS Organizations. Para obtener más información, consulteElementos de política JSON de: Acciónen laGuía del usuario de IAM.
- Recurso: utilice esta palabra clave para especificar el ARN del recurso al que se aplica la instrucción de la política. Para obtener más información, consulteElementos de política JSON de: Recursoen laGuía del usuario de IAM.
- Condición: utilice esta palabra clave para especificar una condición que se debe cumplir para poder aplicar la instrucción de la política.`Condition`normalmente especifica circunstancias adicionales que se deben cumplir para aplicar la política. Para obtener más información, consulteElementos de política JSON de: Condiciónen laGuía del usuario de IAM.
- Efecto: utilice esta palabra clave para especificar si la instrucción de la política permite o deniega la acción en el recurso. Si no concede acceso de forma explícita (o permite) un recurso, el acceso se deniega implícitamente. También puede denegar explícitamente el acceso a un recurso; de esta forma, se asegurará de que un usuario no pueda realizar la acción especificada en el recurso especificado, incluso si otra política otorga acceso. Para obtener más información, consulteElementos de política JSON de: Efectoen laGuía del usuario de IAM.
- Principal: en las políticas basadas en identidad (políticas de IAM), el usuario al que se asocia esta política es de forma automática e implícita la entidad principal. En las políticas basadas en recursos, debe especificar el usuario, la cuenta, el servicio o cualquier otra entidad que desee que reciba permisos (se aplica solo a las políticas basadas en recursos). Actualmente, AWS Organizations solo admite políticas basadas en identidad, no en recursos.

Para obtener más información acerca de la sintaxis y descripciones de las políticas de IAM, consulte laReferencia de políticas JSON de IAMen laGuía del usuario de IAM.

Usar políticas basadas en identidad (políticas de IAM) paraAWS Organizations

Como administrador de la cuenta de administración de una organización, puede controlar el acceso aAWSal adjuntar directivas de permisos aAWS Identity and Access Management(usuarios, grupos y roles) dentro de la organización. Cuando concede permisos, decide quién debe obtener los permisos, para qué recursos se obtienen permisos y qué acciones específicas desea permitir en esos recursos. Si los permisos se conceden a un rol, ese rol puede ser asumido por usuarios de otras cuentas de la organización.

De forma predeterminada, un usuario no tiene permisos de ningún tipo. Todos los permisos deben concederse explícitamente mediante una política. Si un permiso no se concede de forma explícita, se deniega implícitamente. Si un permiso se deniega de forma explícita, se invalidan todas las demás políticas que lo permitan. En otras palabras, un usuario solo tiene los permisos que se concedan de forma explícita y que no se denieguen de forma explícita.

Además de las técnicas básicas descritas en este tema, puede controlar el acceso a la organización mediante las etiquetas aplicadas a los recursos de la organización: la raíz de la organización, las unidades organizativas (OU), las cuentas y las directivas. Para obtener más información, consulte Control de acceso basado en atributos con etiquetas yAWS Organizations (p. 318).

Conceder permisos completos de administrador a un usuario

Puede crear una política de IAM que concedaAWS Organizationsa un usuario de IAM de su organización. Para ello, puede usar el editor de políticas JSON en la consola de IAM.

Para utilizar el editor de política de JSON para crear una política

1. Inicie sesión en la AWS Management Console y abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En la columna de navegación de la izquierda, elija Policies.

   Si es la primera vez que elige Policies (Políticas), aparecerá la página Welcome to Managed Policies (Bienvenido a políticas administradas). Elija Get Started.
3. En la parte superior de la página, seleccione Crear política.
4. Seleccione la pestaña JSON.
5. Introduzca el siguiente documento de política JSON:

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

6. Elija Review policy (Revisar política).

   Note

   Puede alternar entre las pestañas Visual editor (Editor visual) y JSON en cualquier momento. Sin embargo, si realiza cambios o eligeReview policyen laVisual editor (Editor visual)Por

ejemplo, IAM podría reestructurar su política para optimizarla para el editor visual. Para obtener más información, consulteReestructuración de políticasen laGuía del usuario de IAM.

7. En la páginaReview policy, ingrese unaNombrey una opción opcionalDescripciónPara la política que está creando. Revise la política Summary para ver los permisos concedidos por su política. A continuación, elija Create policy para guardar su trabajo.

Para obtener más información acerca de la creación de una política de IAM, consulteCreación de políticas de IAMen laGuía del usuario de IAM.

Concesión de acceso limitado mediante acciones

Si desea conceder permisos limitados en lugar de todos los permisos, puede crear una política que muestre los permisos individuales que desea permitir en la`Action`de la directiva de permisos de IAM. Tal y como se muestra en el siguiente ejemplo, puede utilizar caracteres comodín (*) para conceder solo los permisos `Describe*` y `List*`, que básicamente proporcionan acceso de solo lectura a la organización.

> **Note**
>
> En una política de control de servicios (SCP), el carácter comodín (*) de un elemento `Action` únicamente puede aparecer solo o al final de la cadena. No puede aparecer al principio o en el medio de la cadena. Por lo tanto, `"servicename:action*"` es válido, pero `"servicename:*action"` y `"servicename:some*action"` no son válidos en las políticas SCP.

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

Para obtener una lista de todos los permisos que se pueden asignar en una política de IAM, consulteAcciones definidas porAWS Organizationsen laGuía del usuario de IAM.

Concesión de acceso a recursos específicos

Además de restringir el acceso a acciones específicas, puede restringir el acceso a entidades específicas de la organización. Los elementos `Resource` de los ejemplos en las secciones anteriores especifican el carácter comodín ("*"), que significa "cualquier recurso al que la acción tenga acceso." En su lugar, puede sustituir el "*" por el Nombre de recurso de Amazon (ARN) de las entidades específicas a las que desea permitir el acceso.

Ejemplo: Concesión de permisos a una sola unidad organizativa

La primera instrucción de la siguiente política concede acceso de lectura a un usuario de IAM a toda la organización, pero la segunda instrucción permite al usuario realizarAWS OrganizationsSolo dentro de una única unidad organizativa especificada. Esto no se extiende a ninguna unidad organizativa infantil. No se concede acceso a la facturación. Tenga en cuenta que esto no le da acceso administrativo a la Cuentas de AWS En la unidad organizativa. Otorga sólo permisos para realizarAWS OrganizationsOperaciones en las cuentas dentro de la unidad organizativa especificada:

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "organizations:*",
      "Resource": "arn:aws:organizations::<masterAccountId>:ou/o-<organizationId>/ou-
<organizationalUnitId>"
    }
  ]
}
```

Obtiene el ID de la unidad organizativa y la organización desde la consola de AWS Organizations o llamando a la API `List*`. El usuario o el grupo al que aplique esta política podrá realizar cualquier acción (`"organizations:*"`) en cualquier entidad que esté directamente contenida en la unidad organizativa especificada. La unidad organizativa se identifica por el Nombre de recurso de Amazon (ARN).

Para obtener más información acerca de los ARN de los distintos recursos, consulteRecursos definidos porAWS Organizationsen laGuía del usuario de IAM.

Otorga la capacidad de habilitar el acceso de confianza a entidades principales de servicio limitadas

Puede utilizar el elemento `Condition` de una instrucción de política para limitar aún más las circunstancias donde se debe aplicar dicha declaración de política.

Ejemplo: Conceder permisos para habilitar el acceso de confianza a un servicio especificado

La siguiente instrucción muestra cómo se puede restringir la capacidad de habilitar el acceso de confianza únicamente a los servicios especificados. Si el usuario intenta llamar a la API con una entidad principal de servicio distinta de la de AWS Single Sign-On, esta política no cumple la condición y se deniega la solicitud:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "organizations:EnableAWSServiceAccess",
            "Resource": "*",
            "Condition": {
                "StringEquals" : {
                    "organizations:ServicePrincipal" : "sso.amazonaws.com"
                }
            }
        }
    ]
}
```

Para obtener más información acerca de los ARN de los distintos recursos, consulteRecursos definidos porAWS Organizationsen laGuía del usuario de IAM.

Control de acceso basado en atributos con etiquetas yAWS Organizations

Control de acceso basado en atributosle permiten usar atributos administrados por el administrador, comoetiquetasadjuntado a ambosAWSRecursos yAWSPara controlar el acceso a dichos recursos. Por ejemplo, puede especificar que un usuario pueda tener acceso a un recurso cuando tanto el usuario como el recurso tengan el mismo valor para una determinada etiqueta.

AWS OrganizationsLos recursos etiquetables incluyen Cuentas de AWS , la raíz, unidades organizativas o políticas de la organización. Al adjuntar etiquetas a recursos de Organizations, puede utilizar esas etiquetas para controlar quién puede tener acceso a esos recursos. Para ello, añada la`Condition`Elementos a suAWS Identity and Access Management(IAM) instrucciones de directiva de permisos que comprueban si ciertas claves de etiqueta y valores están presentes antes de permitir la acción. Esto le permite crear una política de IAM que diga efectivamente «Permitir que el usuario administre solo aquellas unidades organizativas que tienen una etiqueta con una clave`X`y un valor`Y`«o «Permitir que el usuario administre sólo aquellas OU que están etiquetadas con una clave`Z`Que tenga el mismo valor que la clave de etiqueta asociada del usuario`Z`.»

Puede basar su`Condition`prueba en diferentes tipos de referencias de etiquetas en una directiva de IAM.

- Comprobación de las etiquetas asociadas a los recursos especificados en la solicitud (p. 318)
- Comprobación de las etiquetas que se asocian al usuario o rol de IAM que realiza la solicitud (p. 319)
- Compruebe las etiquetas que se incluyen como parámetros en la solicitud (p. 319)

Para obtener más información acerca del uso de etiquetas para el control de acceso en las políticas de, consulteControl del acceso a usuarios y roles de IAM mediante etiquetas de recursos. Para obtener la sintaxis completa de las directivas de permisos de IAM, consulte laReferencia de políticas JSON de IAM

Comprobación de las etiquetas asociadas a los recursos especificados en la solicitud

Cuando realiza una solicitud mediante el comandoAWS Management Console, elAWS Command Line Interface(AWS CLI) o uno de losAWSSDK, especifique a qué recursos desea acceder con esa solicitud. Ya sea que esté intentando enumerar los recursos disponibles de un tipo determinado, leer un recurso o escribir, modificar o actualizar un recurso, especifique el recurso al que se tendrá acceso como parámetro en la solicitud. Dichas solicitudes están controladas por las directivas de permisos de IAM que se adjuntan a los usuarios y roles. En estas directivas, puede comparar las etiquetas adjuntas al recurso solicitado y elegir permitir o denegar el acceso en función de las claves y valores de dichas etiquetas.

Para comprobar una etiqueta adjunta al recurso, haga referencia a la etiqueta en un`Conditional` anteponer el nombre de la clave de la etiqueta con la siguiente cadena:`aws:ResourceTag/`

Por ejemplo, la siguiente política de muestra permite al usuario o función realizar cualquierAWS Organizationsoperacióna menos queese recurso tiene una etiqueta con la clave`department`y el valor`security`. Si esa clave y el valor están presentes, entonces la política deniega explícitamente el`UntagResource`.

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

```
        },
        {
            "Effect" : "Deny",
            "Action" : "organizations:UntagResource",
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "aws:ResourceTag/department" : "security"
                }
            }
        }
    ]
}
```

Para obtener más información acerca de cómo utilizar este elemento, consulteControl del acceso a los recursos deyaws:ResourceTagen laGuía del usuario de IAM.

Comprobación de las etiquetas que se asocian al usuario o rol de IAM que realiza la solicitud

Puede controlar qué puede hacer la persona que realiza la solicitud (entidad principal) en función de las etiquetas asociadas al usuario o rol de IAM de esa persona. Para ello, utilice la`aws:PrincipalTag/`*`key-name`*para especificar qué etiqueta y valor se deben adjuntar al usuario o rol que llama.

En el siguiente ejemplo se muestra cómo permitir una acción solo cuando la etiqueta especificada (`cost-center`) tiene el mismo valor tanto en la entidad que llama a la operación como en el recurso al que tiene acceso la operación. En este ejemplo, el usuario que llama puede iniciar y detener una instancia de Amazon EC2 solo si la instancia está etiquetada con el mismo`cost-center`como usuario.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "ec2:startInstances",
            "ec2:stopInstances"
        ],
        "Resource": "*",
        "Condition": {"StringEquals":
            {"ec2:ResourceTag/cost-center": "${aws:PrincipalTag/cost-center}"}}
    }
}
```

Para obtener más información acerca de cómo utilizar este elemento, consulteControl del acceso para entidades principales de IAMy`aws:PrincipalTag`en laGuía del usuario de IAM.

Compruebe las etiquetas que se incluyen como parámetros en la solicitud

Varias operaciones le permiten especificar etiquetas como parte de la solicitud. Por ejemplo, al crear un recurso, puede especificar las etiquetas que se adjuntan al nuevo recurso. Puede especificar una`Condition`elemento que utiliza`aws:TagKeys`para permitir o denegar la operación en función de si se incluye una clave de etiqueta específica o un conjunto de claves en la solicitud. A este operador de comparación no le importa qué valor contiene la etiqueta. Sólo comprueba si está presente una etiqueta con la clave especificada.

Para comprobar la clave de etiqueta, o una lista de claves, especifique un`Condition`Elemento con la siguiente sintaxis:

```
"aws:TagKeys": [ "tag-key-1", "tag-key-2", ... , "tag-key-n" ]
```

Puede usar`ForAllValues:`para prefaciar al operador de comparación para asegurarse de que todas las claves de la solicitud deben coincidir con una de las claves especificadas en la política. Por ejemplo, la siguiente política de muestra permite cualquier operación de Organizations solo silos tresLas claves de etiqueta especificadas están presentes en la solicitud.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "organizations:*",
        "Resource": "*",
        "Condition": {
            "ForAllValues:StringEquals": {
                "aws:TagKeys": [
                    "department",
                    "costcenter",
                    "manager"
                ]
            }
        }
    }
}
```

También puede utilizar la`ForAnyValue:`para prefaciar a un operador de comparación para asegurarse de que al menos una de las claves de la solicitud debe coincidir con una de las claves especificadas en la política. Por ejemplo, la siguiente política permite una operación de Organizations solo siAl menos unoLas claves de etiqueta especificadas está presente en la solicitud.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "*",
        "Resource": "*",
        "Condition": {
            "ForAnyValue:StringEquals": {
                "aws:TagKeys": [
                    "stage",
                    "region",
                    "domain"
                ]
            }
        }
    }
}
```

Varias operaciones le permiten especificar etiquetas en la solicitud. Por ejemplo, al crear un recurso, puede especificar las etiquetas que se adjuntan al nuevo recurso. Puede comparar un par clave-valor de etiqueta en la política con un par clave-valor incluido en la solicitud. Para ello, haga referencia a la etiqueta en un`Conditional` anteponer el nombre de la clave de la etiqueta con la siguiente cadena:`aws:RequestTag/`*`key-name`*y, a continuación, especifique el valor de etiqueta que debe estar presente.

Por ejemplo, la siguiente directiva de ejemplo deniega cualquier solicitud del usuario o rol para crear un Cuenta de AWS donde a la solicitud le falta el`costcenter`, o proporciona esa etiqueta con un valor distinto de`1`,`2`, o bien`3`.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "organizations:CreateAccount",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/costcenter": "true"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": "organizations:CreateAccount",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "aws:RequestTag/costcenter": [
                        "1",
                        "2",
                        "3"
                    ]
                }
            }
        }
    ]
}
```

Para obtener más información acerca de cómo utilizar estos elementos, consulteaws:TagKeysyaws:RequestTagen laGuía del usuario de IAM.

Registro y monitoreo en AWS Organizations

Como práctica recomendada, debe monitorear su organización para asegurarse de que los cambios queden registrados. Esto permite investigar cualquier modificación inesperada y revertir los cambios no deseados. AWS Organizations actualmente admite dos servicios de AWS que permiten monitorear la organización y la actividad que allí se produce.

Temas

Registrar llamadas a la API de AWS Organizations con AWS CloudTrail

AWS Organizations se integra con AWS CloudTrail, un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un servicio de AWS en AWS Organizations. CloudTrail captura todas las llamadas a la APIAWS OrganizationsComo eventos, incluidas las llamadas desdeAWS Organizationsy de las llamadas de código aAWS OrganizationsAPI. Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3, incluidos los eventos deAWS Organizations. Si no configura un registro de seguimiento, puede ver los eventos más recientes en la consola de CloudTrail en el Event history (Historial de eventos). Mediante la información recopilada por CloudTrail, puede determinar la solicitud que se realizó aAWS Organizations, la dirección IP desde la que se realizó, quién la realizó, cuándo y detalles adicionales.

Para obtener más información sobre CloudTrail, consulte laAWS CloudTrailGuía del usuario.

Important

Puede ver toda la información de CloudTrailAWS OrganizationsSólo en la región EE.UU. Este (Norte de Virginia). Si no veAWS Organizationsen la consola de CloudTrail, configure la consola enEE.UU. Este (Norte de Virginia)mediante el menú de la esquina superior derecha. Si consulta CloudTrail con la opciónAWS CLIo las herramientas de los SDK, dirija su consulta al punto de enlace EE.UU. Este (Norte de Virginia).

AWS OrganizationsInformación de en CloudTrail

CloudTrail está habilitado en su Cuenta de AWS Cuando crea la cuenta de. Cuando se produce actividad enAWS Organizations, dicha actividad se registra en un evento de CloudTrail junto conAWSServicios deHistorial de eventos. Puede ver, buscar y descargar los últimos eventos de Cuenta de AWS . Para obtener más información, consulte Ver eventos con el historial de eventos de CloudTrail.

Para obtener un registro continuo de los eventos de Cuenta de AWS , incluidos los eventos paraAWS Organizations, cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. Cuando el registro de CloudTrail está habilitado en su Cuenta de AWS , las llamadas al API realizadas aAWS Organizationsse hace un seguimiento de las acciones de en los archivos de registro de CloudTrail, donde se registran junto con otrosAWSregistros de servicio. Puede configurar otrosAWSpara analizar y actuar según los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- Consulte Servicios e integraciones compatibles con CloudTrail.
- Configuración de notificaciones de Amazon SNS para CloudTrail

All (Todos)AWS OrganizationsLas registra CloudTrail y se documentan enAWS OrganizationsReferencia de la API. Por ejemplo, las llamadas a`CreateAccount`(incluido el`CreateAccountResult`evento),`ListHandshakesForAccount`,`CreatePolicy`, y`InviteAccountToOrganization`genera entradas en los archivos de registro de CloudTrail.

Cada entrada de registro contiene información sobre quién generó la solicitud. La información de identidad del usuario en la entrada de registro le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales raíz o del usuario de IAM
- Si la solicitud se realizó con credenciales de seguridad temporales deRol de IAMo unusuario 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 los archivos de registro de AWS Organizations

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registro en un bucket de Amazon S3 que se especifique. Los archivos log de CloudTrail pueden contener una o varias entradas de log. Un evento representa una solicitud específica realizada desde un origen y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. 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 de entradas de registro de: CreateAccount

En el ejemplo siguiente se muestra una entrada de registro de CloudTrail para`CreateAccount`que se genera cuando se llama a la API y el flujo de trabajo para crear la cuenta comienza a procesarse en segundo plano.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE:my-admin-role",
        "arn": "arn:aws:sts::111122223333:assumed-role/my-admin-role/my-session-id",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAMVNPBQA3EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/my-admin-role",
                "accountId": "111122223333",
                "userName": "my-session-id"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-09-16T21:16:45Z"
            }
        }
    },
    "eventTime": "2018-06-21T22:06:27Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CreateAccount",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.168.0.1",
    "userAgent":  "Mozilla/5.0 (Windows NT 10.0; Win64; x64)...",
    "requestParameters": {
        "tags": [],
        "email": "****",
        "accountName": "****"
    },
    "responseElements": {
        "createAccountStatus": {
            "accountName": "****",
            "state": "IN_PROGRESS",
            "id": "car-examplecreateaccountrequestid111",
            "requestedTimestamp": "Sep 16, 2020 9:20:50 PM"
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```


En el ejemplo siguiente se muestra una entrada de registro de CloudTrail para`CreateAccount`después de que el flujo de trabajo en segundo plano para crear la cuenta se complete correctamente.


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "..."
  },
  "eventTime": "2020-09-16T21:20:53Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CreateAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "....",
  "requestParameters": null,
```

```
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "createAccountStatus": {
      "id": "car-examplecreateaccountrequestid111",
      "state": "SUCCEEDED",
      "accountName": "****",
      "accountId": "444455556666",
      "requestedTimestamp": "Sep 16, 2020 9:20:50 PM",
      "completedTimestamp": "Sep 16, 2020 9:20:53 PM"
    }
  }
}
```

En el ejemplo siguiente se muestra una entrada de registro de CloudTrail que se genera después de`CreateAccount`el flujo de trabajo en segundo plano no puede crear la cuenta.

```
  {
  "eventVersion": "1.06",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2018-06-21T22:06:27Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CreateAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "createAccountStatus": {
      "id": "car-examplecreateaccountrequestid111",
      "state": "FAILED",
      "accountName": "****",
      "failureReason": "EMAIL_ALREADY_EXISTS",
      "requestedTimestamp": Jun 21, 2018 10:06:27 PM,
      "completedTimestamp": Jun 21, 2018 10:07:15 PM
    }
  }
}
```

Entrada de registro de ejemplo: CreateOrganizationalUnit

En el ejemplo siguiente se muestra una entrada de registro de CloudTrail para`CreateOrganizationalUnit`Llame a.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
```

```
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:40:11Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CreateOrganizationalUnit",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "requestParameters": {
        "name": "OU-Developers-1",
        "parentId": "r-a1b2"
    },
    "responseElements": {
        "organizationalUnit": {
            "arn": "arn:aws:organizations::111111111111:ou/o-aa111bb222/ou-
examplerootid111-exampleouid111",
            "id": "ou-examplerootid111-exampleouid111",
            "name": "test-cloud-trail"
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```


Entrada de registro de ejemplo: InviteAccountToOrganization

En el ejemplo siguiente se muestra una entrada de registro de CloudTrail para`InviteAccountToOrganization`Llame a.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:41:17Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "InviteAccountToOrganization",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "requestParameters": {
        "notes": "This is a request for Mary's account to join Diego's organization.",
        "target": {
            "type": "ACCOUNT",
            "id": "111111111111"
        }
    },
    "responseElements": {
        "handshake": {
            "requestedTimestamp": "Jan 18, 2017 9:41:16 PM",
            "state": "OPEN",
            "arn": "arn:aws:organizations::111111111111:handshake/o-aa111bb222/invite/h-
examplehandshakeid111",
            "id": "h-examplehandshakeid111",
```

```
            "parties": [
                {
                    "type": "ORGANIZATION",
                    "id": "o-aa111bb222"
                },
                {
                    "type": "ACCOUNT",
                    "id": "222222222222"
                }
            ],
            "action": "invite",
            "expirationTimestamp": "Feb 2, 2017 9:41:16 PM",
            "resources": [
                {
                    "resources": [
                        {
                            "type": "MASTER_EMAIL",
                            "value": "diego@example.com"
                        },
                        {
                            "type": "MASTER_NAME",
                            "value": "Management account for organization"
                        },
                        {
                            "type": "ORGANIZATION_FEATURE_SET",
                            "value": "ALL"
                        }
                    ],
                    "type": "ORGANIZATION",
                    "value": "o-aa111bb222"
                },
                {
                    "type": "ACCOUNT",
                    "value": "222222222222"
                },
                {
                    "type": "NOTES",
                    "value": "This is a request for Mary's account to join Diego's
 organization."
                }
            ]
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```


Entrada de registro de ejemplo: AttachPolicy

En el ejemplo siguiente se muestra una entrada de registro de CloudTrail para`AttachPolicy`Llame a. La respuesta indica que la llamada ha dado un error porque el tipo de política solicitado no está habilitado en la raíz donde se ha intentado adjuntar la solicitud.


```
{
    "eventVersion": "1.06",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
```

```
    },
    "eventTime": "2017-01-18T21:42:44Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "AttachPolicy",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "errorCode": "PolicyTypeNotEnabledException",
    "errorMessage": "The given policy type ServiceControlPolicy is not enabled on the
 current view",
    "requestParameters": {
        "policyId": "p-examplepolicyid111",
        "targetId": "ou-examplerootid111-exampleouid111"
    },
    "responseElements": null,
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

Amazon CloudWatch Events

AWS Organizationspuede operar con CloudWatch Events para iniciar eventos cuando se producen las acciones especificadas por el administrador en una organización. Por ejemplo, por la sensibilidad de ese tipo de acciones, la mayoría de los administradores desean que se les advierta cada vez que alguien crea una nueva cuenta en la organización o que un administrador de una cuenta miembro intenta salir de la organización. Puede configurar reglas de Events de CloudWatch que buscan estas acciones y, cuando las detectan, envían los eventos generados a los objetivos definidos por el administrador. Los objetivos pueden ser un tema de Amazon SNS que envíe un correo electrónico o un mensaje de texto a sus suscriptores. O bien una función AWS Lambda creada para registrar los detalles de la acción, de modo que pueda revisarlos más adelante.

Para obtener un tutorial que muestra cómo habilitar CloudWatch Events para monitorear la actividad clave de la organización, consulteTutorial: Monitoreo de cambios importantes en la organización con CloudWatch Events (p. 18).

Para obtener más información sobre los eventos de CloudWatch, incluido cómo configurarlo y habilitarlo, consulte laGuía del usuario de Amazon CloudWatch Events.

Validación de la conformidad en AWS Organizations

Auditores externos evalúan la seguridad y la conformidad deAWScomo parte de múltiplesAWSprogramas de conformidad, como SOC, PCI, FedRAMP e HIPAA.

Para saber siAWS Organizationsu otrosAWSse incluyen en un programa de conformidad específico, consulteAWSServicios de conformidad en el ámbito del programa de conformidad. 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 informes en AWS Artifact.

Su responsabilidad de cumplimiento al usar servicios de AWS está determinada por la sensibilidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y regulaciones aplicables. AWS proporciona los siguientes recursos para ayudar con 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 enAWSque se centran en la seguridad y el cumplimiento normativo.
- Documento técnico sobre arquitectura para Seguridad y conformidad HIPAA— Este documento técnico describe cómo las empresas pueden utilizarAWSpara crear aplicaciones que se ajusten al estándar HIPAA.

  Note

  No todos los servicios cumplen con la HIPAA.
- AWSRecursos de conformidad: es posible que este conjunto de guías y libros de ejercicios se apliquen a su sector y ubicación.
- Evaluación de recursos con reglasen laAWS ConfigGuía para desarrolladores— ElAWS Configevalúa en qué medida las configuraciones de los recursos cumplen las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub— EstoAWSproporciona una visión completa de su estado de seguridad dentro deAWSque puede ayudarlo a verificar el grado de conformidad con las prácticas recomendadas y los estándares sectoriales.
- AWS Audit Manager— EstoAWSle ayuda a auditar continuamente suAWSpara simplificar la forma en que gestiona los riesgos y el cumplimiento de las regulaciones y los estándares del sector.

Resiliencia en AWS Organizations

LaAWSLa infraestructura global de está constituida por Regiones de AWS Zonas de disponibilidad y zonas de disponibilidad Regiones de AWS Las redes 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 zonas de disponibilidad 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 acerca de Regiones de AWS Zonas de disponibilidad y zonas de disponibilidad, consulteAWSInfraestructura global.

Seguridad de la infraestructura de AWS Organizations

Como servicio administrado,AWS Organizationsestá protegido por elAWSprocedimientos de seguridad de red globales de que se describen en elAmazon Web Services: Información general sobre procesos de seguridadDocumento técnico.

UtilizaAWSPuede obtener acceso a las Organizations a través de la red. Los clientes deben admitir Transport Layer Security (TLS). Le recomendamos TLS 1.2 o una versión posterior. Los clientes también deben ser compatibles con conjuntos de cifrado con confidencialidad directa total (PFS) tales como Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

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 enlace de FIPS. Para obtener más información acerca de los puntos de enlace de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Referencia de AWS Organizations

Consulte los temas de esta sección para encontrar información de referencia detallada de distintos aspectos de AWS Organizations.

Temas

Cuotas para AWS Organizations

En esta sección se especifican las cuotas que afectan a AWS Organizations.

Directrices de nomenclatura

A continuación se indican las directrices para los nombres que crea en AWS Organizations, incluidos los nombres de cuentas, unidades organizativas (OU), raíces y políticas:

- Deben contener caracteres Unicode
- La longitud máxima de cadena para los nombres varía según el objeto. Para ver el límite real de cada uno de ellos, consulte laAWS OrganizationsReferencia de la APIy busque la operación de API que crea el objeto. Mira los detalles de esa operación`Name`Parámetro de. Por ejemplo: Nombre de cuenta, o bienNombre de OU.

Valores mínimos y máximos

Los siguientes son los ejemplos depredeterminadamáximos para entidades enAWS Organizations.

> **Note**
>
> Puede solicitar un aumento deSOMEde estos valores mediante elService Quotas de consola. Las Organizations son un servicio global que se aloja físicamente en la región EE. UU. Este (Norte de Virginia) (`us-east-1`). Por lo tanto, debe utilizar`us-east-1`Para acceder a cuotas de Organizations cuando se utiliza la consola Service Quotas, la opciónAWS CLI, o unAWSSDK.

Número de Cuentas de AWS En una organización	4 Número máximo de cuentas permitidas en una organización de forma predeterminada. Una invitación enviada a una cuenta computa para esta cuota. La cuenta se devuelve si la cuenta invitada rechaza la invitación, la cuenta de administración cancela la invitación o la invitación caduca.
Número de nodos raíz en una organización	1

Número de unidades organizativas de una organización	1 000
Número de políticas de cada tipo en una organización	1 000 por tipo de política
Tamaño máximo de un documento de política	Políticas de control de servicios: 5120 bytes(no caracteres) Políticas de exclusión de servicios de IA: 2500 caracteres Políticas Backup de seguridad: 10 000 caracteres Políticas de etiqueta: 10 000 caracteres Nota: Si guarda la directiva mediante el comandoAWS Management ConsoleSe elimina el espacio en blanco adicional (como espacios y saltos de línea) entre elementos JSON y fuera de comillas. Si guarda la directiva mediante una operación de SDK o elAWS CLI, la política se guarda exactamente como usted proporcionó y no se produce la eliminación automática de caracteres.
Anidación máxima de OU en un nodo raíz	Cinco niveles de profundidad de OU bajo un nodo raíz.
Número máximo de intentos de invitación que se pueden realizar en un periodo de 24 horas	20 o el número máximo de cuentas permitidas en su organización, la que sea mayor. Las invitaciones aceptadas no se contabilizan en esta cuota. Tan pronto como se acepta una invitación, puede enviar otra invitación ese mismo día. Si el número máximo de cuentas permitidas en su organización es inferior a 20, obtendrá una excepción de «límite de cuenta superado» si intenta invitar a más cuentas de las que puede contener su organización. Sin embargo, puede cancelar invitaciones y enviar nuevas hasta un máximo de 20 intentos en un día.
Número de cuentas miembro que se pueden crear de forma simultánea	5 — Tan pronto como una finaliza se puede iniciar otra, pero solo puede haber cinco en curso a la vez.
Número de entidades a las que puede asociar una política	Sin límite
Número de etiquetas que se pueden asociar a una cuenta raíz, unidad organizativa o cuenta	50

Tiempo de vencimiento de protocolos de enlace (handshakes)

A continuación se indican los tiempos de espera para los protocolos de enlace en AWS Organizations.

Invitación para unirse a una organización	15 días

Solicitud de habilitar todas las funciones de una organización	90 días
El protocolo de enlace se elimina y ya no aparece en las listas	30 días después de que se complete el protocolo de enlace

Número de políticas que puede asociar a una entidad

Los valores mínimos y máximos dependen del tipo de política y de la entidad a la que asocia la política. En la siguiente tabla se muestra cada tipo de política y el número de entidades a la se puede asociar cada tipo.

> Note
>
> Estos números sólo se aplican a las políticas que están directamente adjuntas a una unidad organizativa o a una cuenta. Las directivas que afectan a una unidad organizativa o cuenta por herencianocuentan contra estos límites.

Tipo de política	Mínimo asociado a una entidad	Máximo adjunto a la raíz	Máximo asociado por unidad organizativa	Máximo asociado por cuenta
Política de control de servicios	1 — Cada entidad debe tenerComo mínimoUn SCP conectado en todo momento. No puede eliminar la última política SCP de una entidad.	5	5	5
Política de exclusión de servicios de IA	0	5	5	5
Política Backup de	0	10	10	10
Política de etiquetas	0	10	10	10

> Note
>
> Actualmente, solo puede tener un nodo raíz en una organización.

Políticas administradas de AWS disponibles para su uso con AWS Organizations

En esta sección se identifican losAWSproporcionadas para su uso para las tareas de administración de su organización. No puede modificar ni eliminar una política administrada por AWS, pero puede asociarla o separarla de entidades de la organización según sea necesario.

AWS OrganizationsPolíticas administradas de para su uso conAWS Identity and Access Management(IAM)

Una política administrada de IAM es proporcionada y mantenida porAWS. Una directiva administrada proporciona permisos para tareas comunes que puede asignar a los usuarios adjuntando la directiva administrada al usuario o objeto de rol de IAM apropiado. No tiene que escribir la política usted mismo, y cuandoAWSactualiza la política según corresponda para admitir nuevos servicios, obtendrá automáticamente e inmediatamente el beneficio de la actualización. Puede ver la lista deAWSPolíticas administradas dePolíticasEn la consola de IAM. UsarPolíticas de filtropara seleccionarAWSadministrado.

Puede usar las siguientes políticas administradas de para conceder permisos a los usuarios de de la organización.

Nombre de la política	Descripción	ARN
AWSOrganizationsFullAccess	Proporciona todos los permisos necesarios para crear y administrar completamente una organización.	arn:aws:iam# aws:policy/ AWSOrganizationsFullAccess
AWSOrganizationsReadOnlyAccess	Proporciona acceso de sólo lectura a la información acerca de la organización. No permite al usuario realizar ningún cambio.	arn:aws:iam# aws:policy/ AWSOrganizationsReadOnlyAccess

Actualizaciones a las OrganizationsAWSPolíticas administradas de

En la tabla siguiente se actualiza aAWSDesde que este servicio comenzó a realizar el seguimiento de estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en laAWS OrganizationsPágina Historial de revisión (p. 343).

Cambio	Descripción	Fecha
AWSOrganizationsFullAccess— actualizado para permitir la creación de una organización.	Las Organizations agregaron el`CreateServiceLinkedRole`a la directiva para habilitar la creación de la función vinculada al servicio necesaria para crear una organización. El permiso está restringido a la creación de un rol que sólo puede ser utilizado por el`organizations.amazonaws.com`Servicio	21 de julio de 2021

Políticas de control de servicios administradas por AWS Organizations

Políticas de control de servicios (SCP) (p. 108)son similares a las políticas de permisos de IAM, pero son una característica deAWS Organizationsen lugar de IAM. Puede utilizar las SCP para especificar los permisos máximos de las entidades afectadas. Puede asociar políticas SCP a nodos raíz, unidades organizativas o cuentas de su organización. Puede crear su propia política o bien usar las políticas que

IAM define. Puede consultar la lista de políticas de su organización en la páginaPolíticasen la consola Organizations.

> **Important**
>
> Cada nodo raíz, unidad organizativa y cuenta debe tener al menos una política SCP asociada en todo momento.

Nombre de la política	Descripción	ARN
FullAWSAccess	ProporcionaAWS OrganizationsAcceso a la cuenta de administración de a las cuentas miembro.	arn:aws:organizations# aws:policy/service_control_policy/P-FullawsAccess

Solución de problemas de AWS Organizations

Si surgen problemas a la hora de trabajar con AWS Organizations, consulte los temas de esta sección.

Temas

Solución de problemas generales

Utilice la información aquí ofrecida para diagnosticar y solucionar los problemas de acceso denegado u otros problemas comunes que puedan surgir al trabajar con AWS Organizations.

Temas

Aparece un mensaje de "acceso denegado" al realizar una solicitud a AWS Organizations

- Compruebe que tiene permisos para llamar a la acción y a los recursos que ha solicitado. Un administrador debe conceder permisos asociando una política de IAM a su usuario de IAM o a un grupo del que sea miembro. Si las instrucciones de la política que conceden esos permisos incluyen alguna condición, como la hora del día o restricciones de direcciones IP, también debe cumplir esos requisitos cuando envíe la solicitud. Para obtener más información sobre cómo consultar o modificar políticas para un usuario, grupo o rol de IAM, consulte.Uso de las políticasen laGuía del usuario de IAM.
- Si va a firmar las solicitudes de la API manualmente (sin usar los SDK de AWS), compruebe que haya firmado correctamente la solicitud.

Aparece un mensaje de "acceso denegado" al realizar una solicitud con credenciales de seguridad temporales

- Compruebe que el usuario o rol de IAM que está utilizando para realizar la solicitud tiene los permisos adecuados. Los permisos de credenciales de seguridad temporales se obtienen de un usuario o rol de IAM, y, por tanto, están limitados a los concedidos al usuario o rol de IAM. Para obtener más información sobre cómo se determinan los permisos de las credenciales de seguridad temporales, consulte.Control de los permisos para credenciales de seguridad temporalesen laGuía del usuario de IAM.
- Compruebe que las solicitudes se han firmado correctamente y que la solicitud tiene el formato correcto. Para obtener más información, consulte laconjunto de herramientaspara el SDK elegido oUso de credenciales de seguridad temporales para solicitar acceso aAWSRecursosen laGuía del usuario de IAM.
- Compruebe que sus credenciales de seguridad temporales no hayan caducado. Para obtener más información, consulteSolicitud de credenciales de seguridad temporalesen laGuía del usuario de IAM.

Obtengo un mensaje de «acceso denegado» cuando intento dejar una organización como cuenta miembro o eliminar una cuenta miembro como cuenta de administración

- Puede eliminar una cuenta miembro solo después de habilitar el acceso de usuario de IAM a facturación en la cuenta miembro. Para obtener más información, consulteActivación del acceso a la consola de Billing and Cost Managementen laAWS Billing and Cost ManagementGuía del usuario.
- Puede eliminar una cuenta de su organización solo si la cuenta tiene la información que necesita para funcionar como cuenta independiente. Cuando crea una cuenta en una organización con la consola, la API o los comandos de la AWS CLI de AWS Organizations, dicha información no se recopila automáticamente. Por cada cuenta que desee convertir en independiente, deberá aceptar el Acuerdo de cliente de AWS, elegir un plan de soporte, proporcionar y verificar la información de contacto necesaria y proporcionar un método de pago. AWS utiliza el método de pago para cobrar cualquier actividad de AWS facturable (no de la capa gratuita de AWS) que se produzca mientras la cuenta no esté asociada a una organización. Para obtener más información, consulte Abandonar una organización como cuenta miembro (p. 74).

Obtengo un mensaje de "cuota superada" cuando intento agregar una cuenta a mi organización

Existe un número máximo de cuentas que puede tener en una organización. Las cuentas eliminadas o cerradas también se tienen en cuenta en esta cuota.

Una invitación de unión se contabiliza para el número máximo de cuentas de la organización. La cuenta se devuelve si la cuenta invitada rechaza la invitación, la cuenta de administración cancela la invitación o la invitación caduca.

- Antes de cerrar o eliminar un Cuenta de AWS ,Eliminarlo de la organización (p. 71)Para que no siga contando para su cuota.

- ConsulteValores mínimos y máximos (p. 330)Para obtener más información sobre cómo solicitar un aumento de cuota, consulte.

Aparece un mensaje que indica que "esta operación requiere un periodo de espera" al añadir o eliminar cuentas

Algunas acciones requieren un periodo de espera. Por ejemplo, no se puede eliminar inmediatamente cuentas recién creadas. Vuelva a intentarlo en unos días. Si está teniendo problemas con las cuotas de la cuenta al agregar o eliminar cuentas, consulte.Valores mínimos y máximos (p. 330)Para obtener más información sobre cómo solicitar un aumento de cuota, consulte.

Obtengo un mensaje de "organización todavía inicializando" cuando intento añadir una cuenta a mi organización

Si recibe este error y ha pasado más de una hora desde que se creó la organización, póngase en contacto con AWS Support.

Aparece el mensaje "Invitations are disabled" cuando intento invitar a una cuenta a mi organización.

Esto sucede cuando habilita todas las características en la organización (p. 37). Esta operación puede tardar algún tiempo y requiere que todas las cuentas de miembro respondan. Hasta que se complete la operación, no podrá invitar a nuevas cuentas a unirse a la organización.

Los cambios que realizo no están siempre visibles inmediatamente

Al ser un servicio al que se obtiene acceso a través de equipos de centros de datos de todo el mundo, AWS Organizations utiliza un modelo de computación distribuida llamado consistencia final. Cualquier cambio que realice en AWS Organizations tardará en aparecer en todos los puntos de enlace posibles. Este retraso se debe en parte al tiempo que se tarda en enviar los datos de un servidor a otro o de una zona de replicación a otra. AWS Organizations también usa almacenamiento en caché para mejorar el rendimiento, pero en algunos casos eso puede generar retrasos. Es posible que el cambio no sea visible hasta que se agoten los datos previamente almacenados.

Diseñe sus aplicaciones globales teniendo en cuenta estos posibles retrasos y asegúrese de que funcionan según lo previsto, incluso cuando un cambio realizado en una ubicación no está visible inmediatamente en otra ubicación.

Para obtener más información acerca del modo en que esto afecta a otros servicios de AWS, consulte los siguientes recursos:

- Administración de la consistencia de los datosen laGuía para desarrolladores de bases de datos Amazon Redshift
- Modelo de coherencia de datos de Amazon S3en laAmazon Simple Storage Service Developer Guide
- Ensuring Consistency When Using Amazon S3 and Amazon Elastic MapReduce for ETL Workflows en el blog de big data de AWS

- Coherencia eventual de EC2en laReferencia de API de Amazon EC2.

Solución de problemas de políticas de AWS Organizations

Utilice la información que se indica aquí para diagnosticar y corregir errores comunes en las políticas de AWS Organizations.

Políticas de control de servicios

Políticas de control de servicios (SCP) deAWS Organizationsson similares a las políticas de IAM y tienen una sintaxis común. Esta sintaxis comienza con las reglas de JavaScript Object Notation (JSON). JSON describe un objeto con pares de nombre y valor que componen el objeto. LaGramática de las políticas de IAMse basa en la definición de nombres y valores que tengan significado y puedan ser entendidos por laAWSLos servicios de que usan políticas para conceder permisos.

AWS Organizationsutiliza un subconjunto de la sintaxis y la gramática de IAM. Para obtener más información, consulte Sintaxis de las políticas SCP (p. 124).

Errores de políticas comunes

Más de un objeto de política

Una SCP debe constar de uno y un solo objeto JSON. Los objetos se indican incluyéndolos en llaves { }. Aunque puede anidar otros objetos dentro de un objeto JSON añadiendo llaves ({}) adicionales en el par exterior, una política solo puede contener un par exterior de llaves { }. El siguiente ejemplo es incorrecto porque contiene dos objetos en la parte superior (indicados en *rojo*):

```
{
  "Version": "2012-10-17",
  "Statement":
  {
     "Effect":"Allow",
     "Action":"ec2:Describe*",
     "Resource":"*"
  }
}
{
  "Statement": {
     "Effect": "Deny",
     "Action": "s3:*",
     "Resource": "*"
  }
}
```

Sin embargo, podría satisfacer la intención del ejemplo anterior con el uso de la gramática de políticas correcta. En lugar de incluir dos objetos de política completos, cada uno con su propio elemento `Statement`, puede combinar los dos bloques en un único elemento `Statement`. El elemento `Statement` tiene una matriz de dos objetos como su valor, tal y como se muestra en el ejemplo siguiente:

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource":" *"
    },
    {
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

Este ejemplo no se puede comprimir en una instrucción `Statement` con un solo elemento, porque los dos elementos tienen efectos diferentes. Por lo general, solo puede combinar instrucciones cuando los elementos `Effect` y `Resource` de cada instrucción sean idénticos.

Más de un elemento Statement

Este error podría parecer a simple vista una variante del error de la sección anterior. Sin embargo, es un tipo de error diferente desde el punto de vista sintáctico. En el siguiente ejemplo, solo hay un objeto de política indicado por un único par de llaves { } en el nivel superior. Sin embargo, ese objeto contiene dos elementos `Statement` en su interior.

Una SCP debe contener solo un elemento `Statement`, que consta del nombre (`Statement`) que aparece a la izquierda de un carácter de punto y coma, seguido de su valor a la derecha. El valor de un elemento `Statement` debe ser un objeto, identificado por llaves { }, que contiene un elemento `Effect`, un elemento `Action` y un elemento `Resource`. El siguiente ejemplo es incorrecto porque contiene dos elementos `Statement` en el objeto de política:

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "ec2:Describe*",
    "Resource": "*"
  },
  "Statement": {
    "Effect": "Deny",
    "Action": "s3:*",
    "Resource": "*"
  }
}
```

Como un objeto de valor puede ser una matriz de varios objetos de valor, puede resolver este problema combinando los dos elementos `Statement` en un elemento con una matriz de objetos, tal y como se muestra en el ejemplo siguiente:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource":"*"
    },
    {
      "Effect": "Deny",
      "Action": "s3:*",
```

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

El valor del elemento `Statement` es una matriz de objetos. La matriz del ejemplo se compone de dos objetos, cada uno de los cuales es un valor correcto para un elemento `Statement`. Cada objeto de la matriz está separado por comas.

El documento de política supera el tamaño máximo

El tamaño máximo de un documento de SCP es 5.120 bytes. Este tamaño máximo incluye todos los caracteres, incluido el espacio en blanco. Para reducir el tamaño de su SCP, puede eliminar todos los caracteres de espacio en blanco (como espacios y saltos de línea) que estén fuera de las comillas.

Llamar a la API mediante solicitudes de consulta HTTP

Esta sección contiene información general acerca del modo de utilizar la API de consulta de AWS Organizations. Para obtener más información acerca de las operaciones y los errores de la API, consulte laAWS OrganizationsReferencia de la API.

> Note
>
> En lugar de realizar llamadas directas a la API de consultas de AWS Organizations, puede utilizar uno de los SDK de AWS. 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 acceso mediante programación a AWS Organizations y AWS. 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.

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

La respuesta es un documento XML. Para obtener más información acerca de la respuesta, consulte las páginas de cada acción en laAWS OrganizationsReferencia de la API.

Temas

Endpoints

AWS Organizationstiene un único punto de enlace de API global alojado en la región de EE.UU. Este (Norte de Virginia).

Para obtener más información acerca deAWSendpoints y regiones para todos los servicios, consulteRegiones y puntos de enlace deen laAWSReferencia general de.

HTTPS obligatorio

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

Firma de solicitudes API de AWS Organizations

Las solicitudes deben firmarse con un ID de clave de acceso y una clave de acceso secreta. Recomendamos encarecidamente que no utilice las credenciales de la cuenta raíz de AWS para trabajar con AWS Organizations. Puede utilizar las credenciales de un usuario de IAM o credenciales temporales como las que usa con un rol de IAM.

Para firmar las solicitudes de la API, debe utilizar Signature Version 4 de AWS. Para obtener más información cómo usar Signature Version 4, consulte Proceso de firma Signature Version 4 en la Referencia general de AWS.

AWS Organizations no es compatible con versiones anteriores, como Signature Version 2.

Para obtener más información, consulte los siguientes temas:

- AWSCredenciales de seguridad de: ofrece información general acerca de los tipos de credenciales que puede utilizar para tener acceso a.AWS
- Prácticas recomendadas de IAMOfrece sugerencias acerca de cómo utilizar el servicio de IAM para ayudar a proteger suAWSrecursos, incluidos los deAWS Organizations
- Credenciales temporalesDescribe cómo crear y utilizar credenciales de seguridad temporales.

Historial de revisión de AWS Organizations

En la tabla siguiente se describen las actualizaciones principales de la documentación de AWS Organizations.

- Versión de API: 11/2016

update-history-change	update-history-description	update-history-date
Se actualizó la directiva administrada de AWSOrganizationsFullAccess para habilitar la creación de una organización.	La directiva administrada se actualizó para permitir la creación de una organización agregando el permiso necesario para crear el rol vinculado al servicio que necesita una organización nueva.	21 de julio de 2021
Integración de Organizations conAWS Configahora admite la acumulación de datos de varias cuentas y regiones.	Puede utilizar una cuenta de administrador delegada para agregar la configuración de recursos y los datos de conformidad de todas las cuentas de miembros de su organización. Para obtener más información, consulteAcumulación de datos de varias cuentas y regionesen la AWS Config Guía para desarrolladores.	16 de junio de 2021
Integración de Organizations conAWS Firewall Managerahora incluye soporte para un administrador delegado.	Ahora puede designar una cuenta de miembro de su organización para que sea el administrador de Firewall Manager de toda la organización. Esto permite una mejor separación de los permisos de la cuenta de administración de la organización.	30 de abril de 2021
Las políticas de backup de las Organizations ahora admiten backup continuo.	Puede utilizar elAWS Backupcon las políticas de copia de seguridad de su organización.	10 de marzo de 2021
Integración de Organizations conAWS CloudFormationStackSets ahora incluye la compatibilidad con un administrador delegado.	Ahora puede designar una cuenta de miembro de su organización para que sea laAWS CloudFormationStackSets administrador para toda la organización. Esto permite una mejor separación de los permisos de la cuenta de administración de la organización.	18 de febrero de 2021

Continúe invitando a cuentas mientras habilita todas las funciones	AWSha actualizado el proceso para habilitar todas las características de una organización. Ahora puede seguir invitando a nuevas cuentas a unirse a su organización mientras espera a que las cuentas existentes respondan a sus invitaciones.	3 de febrero de 2021
Presenta la versión 2.0 delAWS Organizationsconsole (p. 343)	AWSintrodujo una nueva versión delAWSconsola de . Toda la documentación de se ha actualizado para reflejar la nueva forma de realizar las tareas.	21 de enero de 2021
Ahora las Organizations admiten la integración con. AWS Marketplace	Ahora puede habilitar el AWS Marketplace Para compartir las licencias de software de todas las cuentas de su organización de manera más sencilla.	3 de diciembre de 2020
Las Organizations ahora admiten la integración con Amazon S3 Lens	Amazon S3 Lens admite el acceso de confianza y el administrador delegado con las Organizations. Para obtener más información, consulte .Amazon S3 Storage Lensen laAmazon Simple Storage Service Developer Guide.	18 de noviembre de 2020
Copias de seguridad entre cuentas	Cuando utiliza directivas de copia de seguridad para realizar copias de seguridad de los recursos de su organización, ahora puede almacenar copias de la copia de seguridad en otros Cuentas de AWS En la organización.	18 de noviembre de 2020
Regiones de AWS ahora admite en ChinaAWS Resource Access Managercomo un servicio de confianza de las Organizations. (p. 343)	Ahora puede usar elAWS RAMcaracterísticas que se integran con las Organizations como un servicio de confianza cuando utiliza Organizations yAWS RAMen China.	18 de noviembre de 2020
Ahora las Organizations admiten la integración con. AWS Security Hub	Puede habilitar Security Hub en todas las cuentas de su organización y designar una de las cuentas de miembro de su organización como la cuenta de administrador delegada para Security Hub.	12 de noviembre de 2020

Se ha cambiado el nombre de la cuenta maestra (p. 343)	AWS Organizationscambió el nombre de la «cuenta maestra» a «cuenta de gestión». Solo se cambia el nombre y no se cambia su funcionalidad.	20 de octubre de 2020
Sección Nuevas prácticas recomendadas y temas	Se ha añadido una nueva sección para las prácticas recomendadas paraAWS Organizations. La nueva sección incluye temas que tratan las prácticas recomendadas para los usuarios raíz de cuentas de administración y cuentas de miembro y administración de contraseñas.	6 de octubre de 2020
Añadida nueva sección de prácticas recomendadas y dos primeras páginas	Hay una nueva sección para temas que describen las prácticas recomendadas paraAWS Organizations. Esta actualización incluye un tema sobre prácticas recomendadas para la cuenta de administración de una organización y un tema sobre prácticas recomendadas para cuentas de miembro.	2 de octubre de 2020
Las directivas de copia de seguridad de las Organizations ahora admiten copias de seguridad coherentes con las aplicaciones en instancias de Windows EC2 mediante VSS (Volume Shadow Copy Service).	Las políticas Backup de seguridad admiten un nuevo`advanced_backup_settings`«sección. La primera entrada de esta nueva sección es un`ec2`llamada`WindowsVSS`Puede habilitar o deshabilitar. Para obtener más información, consulte .Creación de una Backup de seguridad de Windows habilitada para VSSen laAWS BackupGuía para desarrolladores.	24 de septiembre de 2020
Las Organizations admiten el control de acceso basado en etiquetas y etiquetas	Puede añadir etiquetas a los recursos de las Organizations al crearlas. Puede usar elPolíticas de etiquetaspara estandarizar el uso de etiquetas en los recursos de las Organizations. Puede usar elDirectivas de IAM para restringir el acceso sólo a los recursos que tienen claves de etiqueta y valores especificados.	15 de septiembre de 2020
Se ha añadidoAWS HealthComo servicio de confianza.	Puede agregarAWS HealthEventos en todas las cuentas de la organización.	4 de agosto de 2020

Políticas de exclusión en los servicios de Inteligencia artificial (IA)	Puede usar las políticas de exclusión de servicios de IA para controlar siAWSLos servicios de IA pueden almacenar y utilizar el contenido del cliente procesado por dichos servicios (contenido de IA) para el desarrollo y la mejora continua deAWSServicios y tecnologías de inteligencia artificial.	8 de julio de 2020
Se agregaron políticas de backup e integración conAWS Backup.	Puede usar políticas de copia de seguridad para crear y aplicar políticas de copia de seguridad en todas las cuentas de su organización.	24 de junio de 2020
Support la administración delegada de IAM Access Analyzer.	Le permite delegar el acceso administrativo de Access Analyzer de su organización en una cuenta miembro designada.	30 de marzo de 2020
Integración con AWS CloudFormation StackSets	Puede crear un conjunto de pilas administradas por servicios para implementar instancias de pila en cuentas administradas por AWS Organizations.	11 de febrero de 2020
Integración con Compute Optimizer	Compute Optimizer se ha agregado como un servicio que puede funcionar con las cuentas de su organización.	4 de febrero de 2020
Políticas de etiquetas	Puede utilizar las políticas de etiquetas para ayudar a estandarizar las etiquetas en todos los recursos en las cuentas de su organización.	26 de noviembre de 2019
Integración con Systems Manager	Puede sincronizar los datos de las operaciones entre todos los Cuentas de AWS en su organización en el Explorador de Systems Manager.	26 de noviembre de 2019
aws:principalOrgPaths	La nueva clave de condición de condición global de laAWS Organizationspara el usuario de IAM, el rol de IAM o Cuenta de AWS usuario raíz que está realizando la solicitud.	20 de noviembre de 2019
Integración con reglas de AWS Config	Puede usar elAWS ConfigOperaciones de la API para la administraciónAWS ConfigReglas en todos los Cuentas de AWS En la organización.	8 de julio de 2019

Nuevo servicio para el acceso de confianza	Service Quotas se ha añadido como un servicio que puede funcionar con las cuentas de su organización.	24 de junio de 2019
Integración con AWS Control Tower	AWS Control Tower se ha añadido como un servicio que puede funcionar con las cuentas de su organización.	24 de junio de 2019
Integración de con AWS Identity and Access Management	IAM proporciona datos del último acceso de las entidades de su organización (la organización raíz, las unidades organizativas y las cuentas) al servicio. Puede utilizar estos datos para restringir el acceso a solo los servicios de AWS que necesita.	20 de junio de 2019
Etiquetado de cuentas	Puede aplicar etiquetas a su organización y eliminar estas etiquetas, así como ver las etiquetas de una cuenta de su organización.	6 de junio de 2019
Los recursos, las condiciones y el elemento `NotAction` en las políticas de control de servicios (SCP)	A partir de ahora, puede especificar recursos, condiciones y el elemento `NotAction` en las SCP para denegar el acceso a las cuentas de su organización o unidad organizativa (OU).	25 de marzo de 2019
Servicios nuevos para el acceso de confianza	AWS License Manager y AWS Service Catalog se han añadido como servicios que pueden funcionar con las cuentas de su organización.	21 de diciembre de 2018
Servicios nuevos para el acceso de confianza	AWS CloudTrail y AWS RAM se han añadido como servicios que pueden funcionar con las cuentas de su organización.	4 de diciembre de 2018
Nuevo servicio para el acceso de confianza	AWS Directory Service se ha añadido como un servicio que puede funcionar con las cuentas de su organización.	25 de septiembre de 2018
Verificación de dirección de correo electrónico	Para poder invitar a cuentas existentes a su organización, debe verificar que es el propietario de la dirección de correo electrónico asociada a la cuenta de administración.	20 de septiembre de 2018
Notificaciones CreateAccount	`CreateAccount`Las notificaciones se publican en los registros de CloudTrail de de la cuenta de administración.	28 de junio de 2018

Nuevo servicio para el acceso de confianza	AWS Artifact se ha añadido como un servicio que puede funcionar con las cuentas de su organización.	20 de junio de 2018
Servicios nuevos para el acceso de confianza	AWS Config y AWS Firewall Manager se han añadido como servicios que pueden funcionar con las cuentas de su organización.	18 de abril de 2018
Acceso de servicios de confianza	Ahora puede habilitar o deshabilitar el acceso de determinados servicios de AWS a las cuentas de la organización. AWS SSO es el primer servicio de confianza compatible.	29 de marzo de 2018
Ahora la eliminación de cuentas es un servicio autónomo	A partir de ahora, puede eliminar cuentas creadas desde AWS Organizations sin ponerse en contacto con AWS Support.	19 de diciembre de 2017
Se ha agregado compatibilidad con el nuevo servicio . AWS Single Sign-On	AWS Organizations ahora admite la integración con AWS Single Sign-On (AWS SSO).	7 de diciembre de 2017
AWS ha agregado una función vinculada al servicio para todas las cuentas de la organización.	Una función vinculada al servicio denominado `AWSServiceRoleForOrganizations` se ha agregado a todas las cuentas de una organización para habilitar la integración entre AWS Organizations y otros servicios de AWS.	11 de octubre de 2017
A partir de ahora, puede eliminar cuentas creadas (p. 343)	Los clientes ya pueden eliminar cuentas creadas en su organización con ayuda de AWS Support.	15 de junio de 2017
Lanzamiento del servicio	Versión inicial de la documentación de AWS Organizations que acompañaba el lanzamiento del nuevo servicio.	17 de febrero de 2017

AWSGlosario

Contiene la más recienteAWSterminología, consulte laAWSGlosarioen laAWSReferencia general de.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.